الجرائم الإلكترونية

دراسة قانونية قضائية مقارنة

مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت

الجريمة الإلكترونية وتصنيفاتها-المجرم المعلوماتي-الفيروسات الإلكترونية-التشريع والجريمة الإلكترونية- القضاء والجريمة الإلكترونية- المحكمة الإلكترونية- القاضى الإلكترونى- الجريمة الإلكترونية فى الوطن العربى- الجريمة الإلكترونية فى الغرب والولايات المتحدة الأمريكية- آليات المواجهة - التعاون الدولى.

الدكتور

عبد العال الديربي

الأستاذ

محمد صادق إسماعيل

خبير فى مجال الجرائم الالكترونية ومكافحة الفساد

الطبعة الأولى

2012

المركز القومي للإصدارات القانونية

51 ش علي عبد اللطيف - الشيخ ريحان - عابدين - القاهرة

Mob: 01115555760 - 01002551696 - 01224900337

Tel:002/02/27959200 - 27964395 - Fax: 002/02/27959200

Email: walied_gun@yahoo.com law_book2003@yahoo.com

www.publicationlaw.com

الجرائم الإلكترونية

دراسة قانونية قضائية مقارنة

مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت

الجريمة الإلكترونية وتصنيفاتها-المجرم المعلوماتى-الفيروسات الإلكترونية- التشريع والجريمة الإلكترونية- القضاء والجريمة الإلكترونية- المحكمة الإلكترونية- القاضى الإلكترونى- الجريمة الإلكترونية فى الوطن العربى- الجريمة الإلكترونية فى الغرب والولايات المتحدة الأمريكية- آليات المواجهة - التعاون الدولى.

الدكتور

عبد العال الديربي

الأستاذ

محمد صادق إسماعيل

خبير فى مجال الجرائم الالكترونية ومكافحة الفساد

الطبعة الأولى

2012

المركز القومي للإصدارات القانونية

54 ش علي عبد اللطيف - الشيخ ريحان - عابدين - القاهرة

Mob: 01115555760 - 01002551696 - 01224900337

Tel:002/02/27959200 - 27964395 - Fax: 002/02/27959200

Email: walied_gun@yahoo.com law_book2003@yahoo.com

www.publicationlaw.com

بسم الـلـه الرحمن الرحيم

﴿ وقل اعملوا فسيرى الـلـه عملكم ورسوله والمؤمنون ﴾[1].

صدق الـلـه العظيم

---

(1) الآية رقم 105 من سورة التوبة.



شكر وتقدير

- نتقدم بخالص الشكر والتقدير للمركز القومي للإصدارات القانونية ...
- على الجهد الذي بذلـه لإخـراج هذا العمل على هذه الصورة المتميزة..
- **ونختص بالشكر السيد/وليد مصطفى**

رئيس مجلس الإدارة

- راجين له التوفيق فيما ينشره المركز من إصدارات تسهم في نشر الثقافة والمعرفة القانونية.

الدكتور
عبد العال الديربي

الأستاذ
محمد صادق إسماعيل

بسم الـلـه الرحمن الرحيم

مقدمة

منذ ظهر الحاسب الآلي عام 1946 على يد العالمين الأمريكيين(e.p.eckert_j.w.mauchly) في جامعة بنسلفانيا وشاع استخدامه في العالم بعد ذلك إلي أن وصل إلي العالم العربي في مطلع الستينات على يد الشركات الأجنبية وعدد من المصارف، فإن العالم أصبح في مواجهة كائن ميكانيكي جديد بدأ يغزو الحياة بشكل تدريجي وتطور مطرد في شكل ثورة علمية جديدة، جعلت هذا الحاسب يؤدي من المهـام والوظائـف والتعامل مـع المعلومات والوظائف، مالا طاقة لآلاف الأشخاص بها، وأصبح هذا الجهاز مستودع أسرار الناس وأبحاثهم وخططهم، وغدا الحاكم الآمر والموجه الأمين، لآلات المصانع والمعامل، والمتحكم في حركة الطائرات، والقاطرات ، والمنظم لعمل البنوك والشركات، والمنجز لمهام وأعمال وخدمات الحكومات.

من هنا يمكن القول بأن العالم أصبح أمام ثورة حقيقية هي ثورة المعلومات، أو العالم الرقمي، وصار الناس أحيانا مختارين وفي أحايين أخرى مضطرين للتعامل مع هذا العالم الجديد أو مجتمع المعلومات كما يحلو للبعض أن يسميه، وما لبث الناس قليلا وهم يفيقون من صدمة ثورة المعلومات الجامحة حتى دهمتهم ثورة جديدة خلقها ذلك التزاوج أو الإتحاد الفريد بين هذا الجهاز وأنظمة الإتصالات الحديثة، لنصل في نهاية القرن

الماضي وبدايات هذا القرن الي ما يسمى التواصل عبر شبكة الأنترنت العالمية، التي حطمت الحدود بين الدول وقصرت المسافات بين الأفراد والجماعات، واختصرت الزمن عبر شبكة لامرئية، أو محسوسة، سميت بشبكة الأنترنت العالمية،أو (الشبكة العنكبوتيه) أو (الفضاء السيبراني) والتي بدأ استعمالها للأمور العسكرية أولا في الولايات المتحدة الأمريكيه منذ عام 1969، وبدأ العالم العربي يتعرف عليها في أواخر الثمانينات وبدأت تنتشر فيه تدريجيا، بل إن الأمر تطور إلى حد الاقتراع من خلال جهاز الكمبيوتر مباشرة.

وبعيدا عن الاستخدامات الحميدة أو السلمية للكمبيوتر، يمكن القول بأن التطور المذهل فى هذا المجال، قد ترتب عليه نشوء جرائم ناتجة عن استخداماته المتعددة، وهذه الجرائم إما أن تقع على الكمبيوتر ذاته، وإما أن تقع بواسطة الكمبيوتر حيث يصبح أداة في يد الجاني يستخدمه لتحقيق أغراضه الإجرامية.

ونظرا لازدياد الجرائم المتعلقة بالكمبيوتر شرعت الدول المتمدينة بوضع تشريعات جنائية خاصة لمكافحة جرائم الكمبيوتر التي تعتبر ظاهرة مستحدثة علي علم الإجرام ومن هذه الدول، الولايات المتحدة الأمريكية وفرنسا وباقى دول الاتحاد الأوروبي الذي وضع اتفاقية حول جرائم الكمبيوتر سنة 2001م، والتي أوصت فيها الدول الأعضاء باتخاذ كافة الإجراءات التشريعية أو غيرها حسب الضرورة لجعل الدخول إلى جميع نظم الكمبيوتر أو أي من أجزائه بدون وجه حق جريمة جنائية بحسب القانون المحلي، كما أوصت هذه الاتفاقية على مجموعة من المبادئ العامة المتعلقة بالتعاون الدولي في مجال الشئون الجنائية، وحددت كذلك الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول الأعضاء في غياب الاتفاقيات الدولية.

وهكذا وجد العالم نفسه في قرية صغيرة، وأصبحت قرية المعلومات هذه محط انظار جميع أصحاب المصالح المشروعة وغير المشروعة، وبدأت تقنية المعلومات تفرز أثارا شاملة على البنية الإدارية والاقتصادية والاجتماعية والسياسية، والثقافية، والقانونية للدول ،ذلك أن كل إختراع علمي لابد ان يفتح افاقا جديدة ويرتب أثاراما كانت قائمة قبل وجوده وانتشاره، وهنا كان لابد للقانون أن يتدخل، كيف لا وهو المنظم بقواعده على اختلاف أنواعها، لجميع مناحى الحياة.

ويشير الباحثون في هذا الصدد إلي أن توقيت ولادة قانون الكمبيوتر، بدأ مع شيوع استعمال الكمبيوتر وانخفاض كلفة استخدامه وذلك في نهاية الستينات ومطلع السبعينات، حيث، كانت أولى التحديات القانونية التي أثارها استخدام الكمبيوتر هي اساءة استخدامه على نحو يضر بمصالح الأفراد والمؤسسات، وخاصة في حقل اساءة التعامل مع البيانات الشخصية المخزنة بالكمبيوترعلى نحو يمس أسرارهم وحياتهم الخاصة وحقهم في الخصوصية، والأمر الثاني هو المسئولية عن الأفعال التي تمثل اعتداء على الأموال والمصالح، وحق الأفراد في المعلومات ذات القيمة الإقتصادية .

وطبقا لما نشره معهد (ستانفورد) في الولايات المتحدة فإن أول محاولة لإساءة استخدام الكمبيوتر كانت عام 1958، ليأتي بعدها موجة ظهور القوانين الوطنية في حقل جرائم الكمبيوتر مع نهاية السبعينات، حيث صدر قانون بالولايات المتحدة لأمريكية عام 1978 سبقه إصدار السويد لقانون في العام 1973 يتعلق بحماية الخصوصية، وهكذا نجد أول موجات التشريع التي حظيت بالاهتمام الدولي في مجال قانون الكمبيوتر كانت منصبة على حماية الخصوصية، وحماية تجميع ومعالجة وتخزين وتبادل البيانات الشخصية، وفي بداية فترة السبعينات أيضا، اتضح الإدراك الكبير لأهمية برامج الكمبيوتر وقيمتها بين عناصر صناعة الكمبيوتر وثار جدل حول موقع

حمايتها، هل هو ضمن حماية برامج الكمبيوتر؟ ام هي تشريعات حماية حقوق المؤلف مع اتفاق الجميع على وجوب حمايتها؟ لنجد دولة مثل الفلبين تصدر في العام 1973 تدابير تشريعية في حقل حماية البرمجيات ،توج ذلك التوجه الجهد الفعال لخبراء المنظمة العالمية للملكية الفكرية (الوايبو) الذين وضعو القواعد النموذجية لحماية برامج الكمبيوتر(حماية الملكية الفكرية لبرامج الكمبيوتر)، والتي كانت من أكثر تشريعات قوانين الكمبيوتر نضجا ووضوحا حسبما يرى الكثير من الباحثين لتأتي بعد ذلك موجة تشريعية ثالثة لتشمل حماية البرمجيات في عقد الثمانينيات.

هذا ويوصف العصر الذي نعيشه بعصر التقنية العالية، عصر وسائل معالجة ونقل المعلومات التي غدت المحدد الاستراتيجي للبناء الثقافي والإنجاز الاقتصادي، وإذا كان خط ميلاد التقنية ونماءها، قد أظهر في البدايات اكتشاف وتطور وسائل التقنية العالية، الحاسب الآلي والاتصال، مستقلة عن بعضها البعض، فإن قطاعات التقنية قد تداخلت وتحقق الدمج المعقد بين الحاسبات الآلية ووسائل الاتصال، وبرز في قضاء التقنية من بين وسائلها الكثيرة، الحاسب الآلي، أداة التحكم بالمعلومات وتجميعها ومعالجتها واختزانها واسترجاعها ونقلها في كافة قطاعات النشاط الإنساني، خاصة النشاط الثقافي والتجاري والصناعي.

ولعله من نافلة القول أن جرائم الحاسب الآلي، هى ظاهرة إجرامية جديدة ومستجدة تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن جريمة الحاسب الآلي التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (بيانات ومعلومات وبرامج بكافة أنواعها).

فجريمة الحاسب الآلي جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات،

وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات.

هذه المعطيات هي موضوع هذه الجريمة وما تستهدفه اعتداءات الجناة، وهذا وحده - عبر دلالته العامة - يظهر مدى خطورة جرائم الحاسب الآلي، فهي تطال الحق في المعلومات، وتمس الحياة الخاصة للأفراد، وتهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري، لذا فإن إدراك ماهية جرائم الحاسب الآلي، منوط بتحليل وجهة نظر الدارسين لتعريفها والاصطلاحات الدالة عليها واختيار أكثرها اتفاقا مع الطبيعة الموضوعية لهذه الجرائم، واستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها وسمات مرتكبيها ودوافعهم.

وقد أثار إحصاء إجراءات تقنية المعلومات تحديات لها وزنها بالنسبة لقانون العقوبات في كل الأنظمة القانونية ويرجع السبب في ذلك إلى الحقيقة التي مؤداها أنه حتى هذه اللحظة، فإن الأشياء المادية والمرئية هي التي تكون محمية بالقوانين الجنائية، وحماية المعلومات والقيم المعنوي الأخرى وإن وجدت منذ فترة زمنية قصيرة إلا أنها حتى منتصف القرن العشرين كانت أقل أهمية، وقد طرأ تغيير جوهري على هذا الموقف أثناء العشر سنوات الأخيرة، حيث أدى تطور المجتمع من مجتمع صناعي إلى مجتمع ما بعد الصناعي، إلى تزايد قيمة المعلومات بالنسبة للاقتصاد والمجتمع والسياسة، فضلا عن الأهمية المتنامية لتقنية المعلومات خلال فترة زمنية قصيرة، وهو الأمر الذى رتب يعرف بقانون المعلومات.

وتنبع أهمية هذه الدراسة من كونها تتناول الثورة المعلوماتية من زاوية الجانب السلبى منها والمتعلق بجرائم المعلوماتية وتأثيره على مكونات المجتمع. وأمام هذا الشكل الجديد من الإجرام لا تبدو قوانين العقوبات الوطنية في حالتها الراهنة كافية أو فعالة على النحو المطلوب أو المرضي فنصوصها والنظريات والمبادئ القانونية التي تتضمنها أو تقف ورائها

موروث بعضها من القرن 19، حيث لم يكن هناك فنيين حينذاك وإنما أصحاب مهن وحرفيين.

وتطبيق بعض هذه القوانين على أشكال جديدة للجرائم التي تستعير من تقنيات الحاسبات الآلية والمعلومات أساليبها، لا يصطدم فقط بصعوبات ناجمة عن الطبيعة الخاصة والخصائص الفنية الفريدة للوسائل المعلوماتية المستخدمة في ارتكابها. وإنما تعترضه كذلك صعوبات رئيسية أخرى مرجعها أن نصوص التجريم التقليدية قد وضعت في ظل تفكير يقتصر إدراكه على الثروة الملموسة والمستندات ذات الطبيعة المادية مما يتعذر معه تطبيقها لحماية القيم غير المادية المتولدة عن المعلوماتية.

والحقيقة التى يجب التأكيد عليها أن وسائل الاتصال لم تخترع الجريمة، بل كانت ضحية لها في معظم الأحوال حيث أن هذه الوسائل تعرضت لسوء الاستغـلال من قبل كثيرين ، ومن الثابت أيضا أن المجرمين وظفوا الاتصال تاريخيا – ضمن أدواتهم المختلفة – لخدمة النشاطات الإجرامية التي يقومون بها. أما الجريمة فهي ذاتها الجريمة في قديم التاريخ، وحديثه، لا يختلف على بشاعتها، وخطرها على المجتمع الإنساني أحد، ولذلك اتفق على مواجهتها، ومن أجلها أقيمت المحاكم، وسنت العقوبات، تستوي في النظرة إليها -كسلوك شاذ - كل الشرائع السماوية، والقوانين الوضعية. وعبر حقب التاريخ المختلفة كانت الظاهرة الإجرامية مرادفة للتجمع الإنساني، تعكس في أساليبها، وأنماطها، أحوال وتطورات المجتمع في مختلف النواحي السياسية، والاقتصادية، والاجتماعية، والثقافية، وغيرها. وفي عصر التقنية، وثورة الاتصالات الحديثة تعقدت الجريمة، وتنوعت أساليبها مستفيدة من التطور التقني في كافة مناحي الحياة، حيث وظف المجرمون هذه المستحدثات التقنية الحديثة في تطوير أساليبهم، بل حتى التقنية ذاتها لم تسلم من الجريمة فمنذ بداياتها ظهر معها ما يعرف بجرائم التقنية، أو الجرائم الإلكترونية التي أخذت أبعادا جديدة مع بداية ثمانينات

القرن الماضي بعد انتشار الحاسبات الشخصية، وتطبيقاتها بشكل جماهيري في مختلف أرجاء العالم. ومع مطلع التسعينات من القرن الماضي ظهرت أنماط حديثة أخرى من الجريمة صاحبت انتشار (شبكة المعلومات العالمية الإنترنت) التي برزت كأسرع وسائل الاتصال الجماهيري نموا في تاريخ وسائل الاتصال.

وإزاء ذلك كان لا بد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم، التي لم تعد تتمركز في دولة معينة، ولا توجه لمجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات، مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات و المواصلات، وتعزيز التعاون بينها واتخاذ تدابير فعالة للحد منها والقضاء عليها ومعاقبة مرتكبيها.

من هنا تاتى أهمية هذا الكتاب الذى نحن بصدده، حيث استقل بمعالجة الجريمة الالكترونية من عدة جوانب من خلال ستة فصول كاملة، تناول الفصل الأول منها جرائم الحاسوب وجرائم الإنترنت وتاريخ تطور كل منهما بينما تناول الفصل الثانى الجريمة المعلوماتية من حيث تعريفها وخصائصها وأسبابها وتصنيفها فيما تناول الفصل الثالث الجريمة الإلكترونية فى مصر والدول العربية وجاء الفصل الرابع ليتحدث عن الجريمة الإلكترونية فى أوروبا والدول الغربية وفى مقدمتها الولايات المتحدة الأمريكية وركز الفصل الخامس بشكل تحليلى مقارن على جرائم الإنترنت فى التشريعات اللاتينية المقارنة، وأخيرا رصد الفصل السادس التعاون الدولى ودوره فى مكافحة جريمة سرقة المعلومات.

المؤلفـــان

القاهـرة

2012

الفصل الأول

جرائم الحاسوب والإنترنت

نتناول هذا الفصل من خلال مبحثين رئيسيين أما المبحث الأول فقد ركز على تعريف الحاسوب والإنترنت، فيما اختص المبحث الثاني بتناول تطور جرائم الحاسوب والانترنت.



المبحث الأول

الحاسوب والانترنت .. مفاهيم أساسية

أولا: تعريف الحاسب[1] Computer

يعرف الحاسب بأنه جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية للتعليمات المعطاة له بسرعات كبيرة تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة وبدرجة عالية الدقة، وله القدرة على التعامل مع كم هائل من البيانات وكذلك تخزينها واسترجاعها عند الحاجة إليها[2]. كما يعرف بأنه مجموعة متكاملة من

---

(1) تعددت الترجمات العربية للاصطلاح الإنجليزي Computer فأطلق عليه أولا العقل الإلكتروني ثم الحاسب الآلي واعتمدت المنظمة العربية للمواصفات والمقاييس اصطلاح الحاسوب وصدر معجم الحاسبات عن مجمع اللغة العربية سنة 1987 بدون إضافة كلمة إلكترونية أو آلية إلى كلمة الحاسبات ولهذا ستستخدم في بحثنا اصطلاح الحاسب فقط وكلمة computer تقابلها في اللغة الفرنسية كلمة ordinateur.

انظر في نشأة الحاسب وتطوره د. محمد فهمي طلبه وآخرين ، الحاسبات الإلكترونية: حاضرها ومستقبلها، موسوعة دلتا كمبيوتر، مطابع الكتاب المصري الحديث، سنة 1992، ص ص 35 -59.

(2) Bohl Marlin: Information processing thir ed. Chicags science Reseatch Associates 1981, and davis gorden B. Mangement Information system conceptual foundations structure and development, New York Megraw Hill, 1974, P.40.

وفي نفس المعنى د. محمد حسام محمود لطفي: الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر، عام 1987، ص6.

الأجهزة التي تعمل مع بعضها البعض بهدف تشغيل (process) مجموعة البيانات الداخلة input data طبقا لبرنامج program تم وضعه مسبقا للحصول على نتائج معينة[1].

ويطلق البعض على الحاسب تعبير المنظم ويعرفه بأنه عبارة عن جهاز أو آلة تتولى معالجة المعطيات المخزونة في الذاكرة الرئيسية في صيغة معلومات تحت إشراف برنامج مخزون[2].

ومن أفضل تعريفات الحاسب التعريف الذي أتت به موسوعة دلتا كمبيوتر في مؤلفها المعنون بالموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، وذلك لشموله جميع الوظائف التي يؤديها الحاسب في الحياة العملية حيث عرفت الحاسب computer بأنه جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال بيانات Data Input أو إخراج معلومات Information output وإجراء عمليات

---

(1) Wetherb James c. and Kickson Gary W. Management system, New York Megraw Hill 1984, P.55.

Rerghis A. Vinuses (computer crime): which computer (UK), P.74-75 Aug 1989.

Computer law practice (UK) response to the law comissions working pager No. 110 computer Misuse Vol. 5, No.5, P.185-189, 1989.

وفي نفس المعنى د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني، دار النهضة العربية، 1992.

Executives Guide to computer Bases Information Systems englewood cliffs N.J.: Prentice: Hall 1984, P.9.

وفي نفس المعنى د. خالد حمدي عبد الرحمن، الحماية القانونية للكيانات المنطقية، رسالة دكتوراه جامعة عين شمس، 1992.

(2) Burch John Relix R Strater and favy Grudnisrki Information system theory and practice, New York Wiley 1979, P.35.

حسابية أو منطقية وهو يقوم بالكتابة على أجهزة الإخراج Output Devices أو التخزين والبيانات يتم إدخالها بواسطة مشغل الحاسب operator عن طريق وحدات الإدخال مثل وحدة المعالجة المركزية (C.P.U centeral processing unit.) التي تقوم بإجراء العمليات الحسابية Arithmatic operations وكذلك العمليات المنطقية logaic operations وبعد معالجة البيانات تتم كتابتها على أجهزة الإخراج output devices مثل الطابعات printers أو وسائط التخزين المختلفة stoorage units وجميع العمليات التي يقوم بها الحاسب تتم في سرعة مذهلة تقترب في بعض الأحيان من سرعة الضوء[1].

ثانيا: المكونات المادية للحاسب Hard Ware:

يمكن تقسيم المكونات المادية الأساسية للحاسب إلى ثلاثة أقسام رئيسية هي وحدة التشغيل ووحدات الإدخال والإخراج ووحدات التخزين[2].

1- وحدة التشغيل (PU) Processing Unit:

تعتبر وحدة التشغيل الجزء الرئيسي في جهاز الحاسب ويطلق عليها البعض بحق عقل الحاسب حيث تتكون من الذاكرة الرئيسية Main memory ووحدة الحساب والمنطق Arithmetic and logic unit ووحدة التحكم control unit ويطلق على وحدة الحساب والمنطق ووحدة

(1) سرعة الضوء تبلغ 300 ألف كيلو متر في الثانية الواحدة. في هذا الشأن:

Lloyd Times electronic commutications Megraw Hill bock company 1979, P.101. John daighes Young nlustrates encyclopedie dictionary of Electronaics parker publishing compnay 1981, P.332.

(2) Zake Rodny your first computer sybex 1980 englewood cliffs N. J. printic Hall, P.27.

التحكم معا اسم وحدة التشغيل المركزية C.P.U central processing unit.) كما يطلق عليها أيضا اسم وحدة المعالجة المركزية[1].

(أ) الذاكرة الرئيسية Main memory:

وهي تتكون من جزأين:

(1) ذاكرة القراءة فقط Read only memory (Rom) وهي الذاكرة التي يتم تخزين البيانات والأوامر بها بصفة دائمة عند تصنيعها وهي تتكون من دوائر إلكترونية مثبتة على شرائح chips ومن خصائصها الاحتفاظ بالبيانات والأوامر المخزونة حتى بعد انقطاع التيار الكهربائي ولذلك يتم تخزين بعض الأوامر اللازمة لبدء تشغيل الجهاز فيها كما تحتوي في بعض الأحيان على برامج معينة ومن خصائصها أيضا أنها لا تقبل تخزين أي بيانات بعد تصنيعها إلا بمعرفة الجهة الصانعة أو المتخصصين باستخدام أجهزة خاصة وهي تستخدم في نظام الحاسب بصفة عامة لقراءة البيانات الموجودة بها فقط[2].

(2) الذاكرة العشوائية أو المؤقتة[3] Random Access Memory (RAM):

وهي الذاكرة العشوائية التي تمكن من الوصول إلى عنوان فيها دون

---

(1) Dologite D. G. Using small business computer englewood cliffs N. J. Prentic Hall 1985, P.37.

وفي نفس المعنى أ. د/ محمد فهمي طلبة وآخرون: المرجع السابق، ص93 إلى ص96، د. هاني كمال مهدي وآخرون، المرجع الشامل لنظام التشغيل Dos موسوعة دلتا كمبيوتر عام 1991، ص21.

(2) Mc Williams Peter A the personal computer book prelude, 1982, P.28.

(3) أ. د/ محمد فهمي طلبة وآخرون: الحاسبات الإلكترونية حاضرها ومستقبلها موسوعة دلتا كمبيوتر، المرجع السابق، ص63.

حاجة إلى المرور على العناوين الأخرى وهي تختلف عن ذاكرة القراءة فقط Rom. حيث أن هذه الأخيرة غير قابلة للتعديل بحسب الأصل بواسطة المستخدم أما الذاكرة العشوائية وتسمى أيضا الذاكرة المؤقتة Temporary memory فإن محتوياتها تتغير حسب البرامج التي يتم تحميلها بالحاسب كما أنها تفقد المعلومات والبيانات المخزونة بها عند انقطاع التيار الكهربائي وقد درج على تسمية الذاكرة العشوائية باسم الذاكرة الرئيسية من معظم العاملين في مجال الحاسبات[1]، كما يطلق عليها أيضا الذاكرة المتطايرة Volatile memory.

(ب) وحدة الحساب والمنطق (Aritmetic and logic unit (ALU:

وحدة الحساب والمنطق هي جزء من وحدة المعالجة المركزية (C.P.U.) متخصص في تأدية العمليات الحسابية مثل الجمع والطرح والضرب والقسمة...الخ. والعمليات المنطقية مثل مقارنة الحروف وتحتوي على سجل خاص Register لتخزين نتائج هذه العمليات أثناء معالجة البيانات وهي تمثل الجزء الرئيسي في عملية معالجة البيانات.

(ج) وحدة التحكم (Control Unit (CU):

وهي جزء من وحدة المعالجة المركزية (CPU) وتقوم بالتنسيق والتحكم في البيانات الداخلة والخارجة من وإلى الذاكرة الرئيسية للحساب بتوجيهها إلى القنوات المختلفة. كما أن وحدة التحكم تعمل كوسيلة اتصال من الذاكرة الرئيسية ووحدة الحساب والمنطق إلى باقي وحدات الحاسب كما أنها تحتوي على ساعة منطقية تقوم بالتحكم في توقيت العمليات المختلفة وتحتوي وحدة التحكم أيضا على وحدات تخزين تسمى

(1) Webster Tony Micro computer butercude Mcgraw Hill, 1983, P.31.

المسجلات registers لا تزيد سعتها عن عدة أحرف Bytes وتؤدي مجموعة من الوظائف الأساسية فهي مثلا تخزن عنوان الأمر التالي المطلوب تنفيذه، ولأنها تمتاز بسرعة التشغيل فإنها تستخدم في تسهيل حركة البيانات بين الذاكرة الرئيسية ووحدة الحساب والمنطق(1).

2- وحدات الإدخال والإخراج **Input / output units**:

وهي التي تستخدم في إدخال البيانات والمعلومات إلى وحدة التشغيل المركزية أو إخراجها لاستخدامها بواسطة المستخدم وذلك بتوجيه من وحدة التحكم.

ثالثا: المكونات المنطقية للحاسب (البرامج) **Software**:

يعرف البرنامج لغويا بأنه: مصطلح يستخدم للدلالة على جميع المكونات غير المادية لنظام الحاسب ويشمل ذلك برامج النظام وهي البرامج اللازمة لتشغيل الحاسب وبرامج التطبيقات وهي البرامج الخاصة بمستخدم الحاسب. ويعرفه بعض الكتاب بأنه تعليمات مكتوبة بلغة ما موجهة إلى جهاز تقني معقد ويسمى بالحاسب الإلكتروني بغرض الوصول إلى نتيجة معينة(2).

ويرى البعض أن الترجمة الدقيقة لاصطلاح software هي اصطلاح الكيان المنطقي حيث يشمل بالإضافة إلى البرنامج الذي هو جوهر الكيان المنطقي كافة الوثائق اللازمة والمصاحبة لهذا البرنامج

(1) انظر Lesson Marjaric computer operations chicago science Research Associates 1983, P.33.

(2) Bohl Marilyn Information processing third ed chicags: sciencs research associates, 1981, P.25.

كذلك سائر البرامج الأخرى المعاونة وكافة العناصر غير المادية اللازمة لتشغيل الحاسب والاستفادة من إمكاناته[1].

وقد عرف القانون الأمريكي الصادر سنة 1980 والخاص بحماية حق المؤلف البرنامج software بأنه مجموعة توجيهات أو تعليمات يمكن للحاسب استخدامها بشكل مباشر أو غير مباشر للوصول إلى نتيجة معينة، وتعرف المنظمة العالمية للملكية الفكرية البرنامج بأنه: مجموعة تعليمات يمكنها إذا ما نقلت على ركيزة تستوعبها الآلة أن تشير تؤدي تساعد في الوصول إلى خاصية ما أو هدف أو نتيجة خاصة بواسطة آلة يمكنها القيام بالتعامل مع المعلومة. أما العاملون في مجال الحاسبات فيطلقون على المكونات المنطقية للحاسب تعبير برنامج بل يطلقون عليها نفس المصطلح الإنجليزي software ويعرفونه بأنه: الأوامر المرتبطة منطقيا والموجهة إلى الحاسب بعد ترجمتها إلى اللغة الوحيدة التي يفهمها وهي لغة الأرقام الثنائية Binary code وهذه البرامج يمكن تصنيفها إلى نوعين: برامج التطبيقات وبرامج النظام.

1- برامج التطبيقات Applications program / software:

وهي البرامج التي تصمم لتنفيذ وظائف محددة إدارية أو علمية.... الخ، مثل المرتبات payroll والدراسات الإحصائية statistical analysis والصناعية Manuactouring والمحاسبة Accounting والعديد من البرامج الأخرى[2].

---

(1) Executivess guide to computer bases information systems englewood cliffs N. J. : prentic Hall 1983, P.12 and jacques clavtez securite informatique etc virus cyrolles 1990, P.3.

(2) د. علاء الدين محمد فهمي وآخرون: عالم الجداول الإلكترونية، موسوعة دلتا كمبيوتر، مطابع الكتب المصري الحديث، 1992، ص26.

2- برامج النظام system program / software:

وهي برامج تعتبر أكثر عمومية من برامج التطبيقات وتكون عادة مستقلة عن أي تطبيق محدد فهي تخدم برامج التطبيقات عن طريق تحقيق أكبر استفادة ممكنة من مكونات الحاسب فمثلا عند بدء تشغيل الحاسب يقوم برنامج معين بتجهيز الأجهزة والمكونات للعمل ومن أهم برامج النظام مترجمات ومفسرات اللغات المختلفة كذلك تدخل نظم التشغيل operating systems ضمن هذا التصنيف.



المبحث الثانى
تطور جرائم الحاسوب والانترنت

تاريخيا أرجع الفقه الجنائي جرائم الحاسوب إلى العام 1960[1]. وأما جرائم الإنترنت فإنه يمكن القول إنها بدأت مع العام 1988 وكانت أول الجرائم التي ترتبط عضويا بالإنترنت هي جرائم العدوان الفيروسي فيما هو معروف في التاريخ القانوني بجريمة دودة موريس المؤخرة واقعتها في 2 الحرث / نوفمبر 1988.

ولا يزال الفقه والتشريع المقارن في حقيقة الأمر يستشعر الحرج في التمييز بين كل من جرائم الحاسوب وبين تلك الناجمة عن استخدام الإنترنت، حتى إن تقرير الأمم المتحدة عن منع الجريمة عام 1995 تبني الموقف المقارن المذكور هذا فصدر عنوان التقرير Computer crimes & other crimes related to computer

لذلك نجد أن تعريف جرائم الحاسوب في الفقه والتشريع يسوده اتجاه يجمع بين الجرائم التي تقع على الحاسوب ذاته وتلك التي يكون الحاسوب وسيلة ارتكابها، فهي لدي هذا الاتجاه تعرف بأنها "فعل غير مشروع يتورط نظام الحاسوب فيه، سواء كان الحاسوب كآلة هو موضوع الجريمة أو كان الوسيلة إلى ارتكابها أو مستودع الدليل المرتبطة بالجريمة". وهو تعريف مستمد من أكثر التعريفات شعبية لجرائم الحاسوب الذي قال به الأستاذ Donn Parker من حيث إن جرائم الحاسوب هي "جرائم تتطلب دراية

---

(1) (SIEBER) Dr. Ulrich – Computer crimes & other crimes related to information technology rev. inter.de droit penal 1991 p. 1033.

ضرورية بالحاسوب لكي يتم ارتكاب الجريمة بنجاح"[1]. ولم تأت الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة 2001/11/23 على تعريف محدد للجريمة عبر الإنترنت[2]، وإنما اعترفت بنوعية من الجرائم يمكن ارتكابها عبر الإنترنت.

ولقد توسعت إدارة العدل الأمريكية في ربط الحاسوب بتقنيته فذهبت إلى تعريف جرائم الحاسوب بأنها "هي كل عدوان بالارتكاب على أي قانون يتضمن في محتواه تقنية الحاسوب ويكون عرضة للتحقيق والاتهام"[3] كان ذلك بالطبع بتأثير من اتجاهات المشرع الأمريكي في تعديل 1996 لقانون البنية الوطنية للمعلومات The National Infrastructure Information Act (القسم 1030)، الذي أستوحي التجريم من الربط بين الحاسوب وتقنيته

(1) Voir site : remp (the royal candian mounted police) " computer crimes is any illegal act which involves a computer systems whether the computer is an obect of crime, an instrument used to commit a crime or a respsitory of evidence related to a crime". Available online in feb. 2000 at: http://www.rcmp.com (mak d. rasch – criminal law and the internet – the internet and association. Copyright © 1996 by the computer law association, inc. p.6, donn parker of sri, is necessary for the successful commission of the offense.

(2) Convention on CyberCrime – Explanatory Report, adopted on 8 Nov. 2001, op. cit.

(3) (SCALION) Robert – crime on the internet, fall 1996, p. 1. "compuer crime is any violation of the law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution" available online in feb. 2000 at : http://wings.buffallo.edu/complaw/complawpapers/scalion.html

- THOUMYRE - abuses in the cyberspace, op cit. P. 7

ككل، فتمخض هذا الاتجاه عن وجود ثلاثة أنواع من الجرائم التي يمكن ارتكابها عر الحاسوب وذلك وفقا للمنهج الأمريكي ، وهي[1] :

أولا : الجرائم التي يكون الحاسوب هدفا لها، وهي نوعية من الجرائم يكون هدف المجرم فيها التوصل إلى سرقة بيانات من الحاسوب أو إحداث إضرار به أو بنظام تشغيله أو بالشبكة التي يعمل خلالها.

ثانيا : الجرائم التي يكون الحاسوب وسيلة لارتكابها، وهذه النوعية من الجرائم تحدث عندما يستخدم المجرم الحاسوب لتسهيل ارتكاب بعض الجرائم التقليدية مثل الاحتيال على البنوك كما لو قام موظف بأحد البنوك باستخدام برمجية تحويل العملة لصالحه فيودع مبالغ محولة لحسابه عوضا عن وضعها في مسارها الصحيح، وكذلك القيام بإعداد Produce أو نقل Transfer أو حيازة Possess آلة Device بما في ذلك الحاسوب بنية استخدامها في تزوير وثائق إثبات شخصية (To Falsify Identification documentation (18 USCode Sec. 1028

ولقد توسعت بعض التشريعات في مدلول مصطلح "أدوات التزوير Forgery Devices" لكي تشمل الحاسوب وملحقاته Equipment وبرمجياته Software إذا أعدت خصيصا بغرض التزوير مثل قانون ولاية نيوجيرسي (N.J.Stat.ANN. Sec. 2 C : 21-1) ،

ثالثا : الجرائم التي يكون فيها الحاسوب أداة لحفظ الأدلة دون أن يكون وسيطا في الحصول عليها، كما هو الحال في قيام مروجي المخدرات

(1) ويلاحظ أن هذا التقسيم كان قد وضعه الأستاذ الدكتور جميل عبد الباقي في مؤلفه - الجرائم الناشئة عن الحاسب الآلي - تقرير مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي - دار النهضة العربية القاهرة 1992.

والاتجار غير المشروع فيها، وكذلك معدي البرمجيات المعتدى على حقوق الملكية فيها وكذلك السرقة الإلكترونية التي تتم عدوانا على حقوق المؤلف بوضع سرقاتهم وملفاتهم وسجلاتهم في الحاسوب.

ومما تجدر الإشارة إليه إن مثل هذا التقسيم السالف ليس جامعا مانعا للتعبير عن جرائم الحاسوب، إذ هناك من الجرائم التي ترتكب بواسطة الحاسوب ومع ذلك لا يمكن إدراجها في أي من الأقسام أو الأشكال الثلاثة مثلما هو الحال في جريمة سرقة وقت الحاسوب مثلا[1] وهي جريمة يعرفها القسم Tit. 18 USCode Sec. 641 من التقنين الأمريكي كجريمة من جرائم المعلوماتية[2].

(1) د. جميل الصغير - الجرائم الناشئة عن استخدام الحاسب الآلي - المرجع السابق ، ص 24.

(2) United States v Sampsonm, 6 COMP, L. SERV. REP. 879 (N.D. Cal. 1978)

ففي هذه القضية فقد اعتبرت المحكمة أن الاستخدام غير المصرح به لحاسوب في مؤسسة حكومية Unauthorized use of computer time يشكل جريمة عدوان على أملاك الحكومة وفق ما هو مقرر في القسم Sec. 641 المشار إليه - انظر كذلك فيما يتعلق بالقسم 641 المذكور :

18 U.S.C. & 641. See : United States v. Friedman. 445 F. 2d 1076, 1087 (9th Cir.) (Theft of grand jury transcripts and information contained therein was theft of government property). Cert. denied. 404 U.S. 958 (1971) : United States v. Morison, 604 F. Supp. 655, 663-65 (D. Md. 1985) ("theft" of classified information supports embezzlement conviction); United States v. DiGillo, 538 F. 2d 972 (3d Cir). Cert. denied. 429 U.S. 871 (1971) (theft by photocopying government secords sufficient to support & 641 convocation) : United States v. MeAusland, 979 F.2d 970 (4th Cir. 1992) (theft of competitior's confidential bid information violates & 641).

وربما يكون السبب في التوسع السالف عائدا إلى أن إمكانيات الحاسوب لم تبرز إلى الوجود بالشكل الذي يجب أن تكون عليه، فكل ما نعلمه عن قدرات الحاسوب يقل كثيرا عما نعلمه عن قدرات الإنترنت. فهذه الأخيرة، وإن كانت لم تأخذ حظها كما ينبغي، فقد تناولها الساسة وفقهاء القانون والاقتصاد على المستوي الإقليمي والدولي بكثير من الـامل وهي بعد في بداياتها، في حين إن مسيرة الحاسوب تبدو هادئة أو طبيعية. ومثل هذا الأمر وجد له تأثير كبير في الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة 2001/11/23 حيث اعترفت الاتفاقية، في المادة الأولى منها، بمصطلح "نظام الحاسوب Computer System" ولم تأخذ في الاعتبار مجرد مصطلح "الحاسوب Computer" فقد حددت الاتفاقية هذا المصطلح بكونه يشمل "أية آلة أو مجموعة مرتبطة فيما بينها أو ذات علاقة من الآلات، يمكن بإضافة برمجية إلى واحد أو أكثر منها، أن تقوم بمعالجة آلية للبيانات"[(1)].

إننا إذن أمام مفارقة بين الحاسوب وبين أحد تقنياته. وهناك ما يميز الأثنين على الرغم من التعميم (الحاسوب) والتخصيص (الإنترنت). وهو تمييز يقوم على أكثر المظاهر بساطة إذ إنه لكي يتم لنا الولوج إلى الحاسوب فإن علينا فقط أن نضغط مفتاح تشغيله، أما الإنترنت فإننا نحتاج، فضلا إلى جهاز حاسوب عامل، إلى الولوج إليها بالاتصال بوسيط هو مزود الإنترنت Provider يمكننا من التعامل مع الخادم Surver وهوة أمر يحتاج إليه خاصة من خلال الحاسوب.

(1) Art. 1 Definitions : "For purposes of this convention : Computer System means any device or a group of inter – connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".

وبدون إحداث اتصال بين الحاسوب وبين الإنترنت عن طريق وسيط – حتى الآن- لا يمكن القول بوجودنا على الإنترنت. وعليه فإن مجرد القول بارتكاب جريمة حاسوب لا يعني ضرورة وجودنا على الإنترنت وإنما يكفي أن يكون الحاسوب في حالة عمل، في حين أنه لا يمكن القول بارتكاب جريمة من جرائم الإنترنت دون أن نكون على الإنترنت Online[1].

ومثل هذا القول نجده في القانون الأمريكي حيث يميز القسم USC Sec. 103018 ، بين مصطلحي حاسوب Computer وبين حاسوب مشمول بالحماية Protected computer، فهذا الأخير يعني ذلك الحاسوب المتصل بغيره عن طريق الشبكات / الإنترنت في حين إن إيراد مصطلح حاسوب Computer فقط فإنه يعني مجرد الحاسوب غير المتصل بأي شبكة ولو داخلية (حيث يعد هنا أداة تخزين فقط).

هذه الخصوصية التي منحها الحاسوب للإنترنت جعلتها تتميز في الحقيقة عنه من حيث الجزئية التي تعمل خلالها، وإذا كان مثار اهتمام رجال القانون في زمننا المعاصر هو التعامل مع تفريع جديد في قانون المعلوماتية Droit Informatique ، هو قانون الإنترنت CyberLaw ، فهذا لا يعني في الحقيقة التعامل مع قانون الحاسوب Computer Law الذي يمثل أحد تفريعات قانون المعلوماتية أيضا.

لذلك فإننا نتجه اتجاها آخر في هذا الشأن حيث نجد أنه من الصواب إحداث فصل في هذا الإطار من حيث تعريفنا لجرائم الإنترنت تعريفا

(1) أن مصطلح Online يثير جدلا حيث أنه بالإنجليزية يشير إلى وجودنا على الإنترنت حيث إن ما يؤخذ في الاعتبار أن النظرة إلى الإنترنت كونها خط مفتوح يلزم لكي نصل إليها أن نكون على هذا الخط في حين أنه إذا كان خارجها فإن المصطلح المستخدم هو Off Line .

منفصلا عن جرائم الحاسوب، باعتبارها جرائم ناجمة عن استخدام الإنترنت، وهو التعريف المبني على فهم عميق لطبيعة المشكلة من حيث ضرورة الفصل بين نوعي هذه الجرائم. حيث إن الإنترنت أفاءت على القانون بأشكال إجرامية جديدة لم تكن معروفة، حتى في ظل التجريم عبر الحاسوب حيث إنه كنتيجة لظهور الإنترنت أضحت المشكلة ليست فقط إحداثيات التمييز في إطار التجريم عبر الحاسوب، في محاولة تتعدى منطق التبسيط إلى التعقيد (مثال جرائم الحاسوب - الجرائم المرتبطة بالحاسوب وتفصيلاتها أيضا ...إلخ) [1]. ولعل ما أنتهي إليه التطور الذي نراه سلبيا في توصيات مؤتمر G8 (الثمانية الكبار) عام 1998 ليدعو إلى مزيد من التأمل في هذا الشأن، إذ تم التوصل إلى مصطلح High- Tech Crime أو جرائم التقنية العالية أو المتقدمة كنوع من محاولة التوسع في جرائم الحاسوب لكي تشمل كافة الجرائم التي يكون الحاسوب طرفا فيها. وهذا كله يجعلنا نقرر أن هناك مفارقة مصطنعة بين جرائم الحاسوب وجرائم الإنترنت، على الرغم من الالتصاق الذي يكاد يكون طبيعيا بينهما.

وهذا الاتجاه الذي نأخذ به يجد له أساسا فقهيا يسعي إلى إقامة بنيانة على النحو الذي يحقق مصلحة الإنسان قبل الآلة، إذ يذهب هذا الاتجاه إلى أن جرائم الإنترنت هي "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير

(1) (KASPERSEN) Prof. Dr. Henrik W. K. – crimes related to the computer network. Threats and opportunities criminological perspective, p. 258. five issues in European criminal justice: corruption, women in the criminal justice system, criminal policy indicators, community crime prevention, and computer crime proccedings of the vi European colloquium on crime and criminal policy Helsinki 10-12 December 1998, European institute or crime prevention and control, affiliated with the united nations (heuni) p. O. Box 161, fin- 00131 Helsinki Finland publication series no. 34

- Thoumyre – abuses in the cyberspace, op. cit., p. 10

المشرع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال المادية والمعنوية[1].

وعلى الرغم من التوجه الصحيح في تعريف جرائم الإنترنت على النحو السالف، سيما هو يوضح لزوم العمد، فكان هذا الرأي سباقا عن اتجاهات الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة 2001/11/23، فإن هذا التعريف لا يخلو من نقد، حيث يستلزم الامتناع كنشاط مادي في مثل هذه الجرائم، وهو الأمر الذي لا يمكن تصوره في هذا الشأن.

وعندنا يمكن وضع تعريف جامع مانع لجرائم الإنترنت إذا أخذنا في الاعتبار ثلاث نقاط رئيسية، وعلى ضوئها يمكن وضع تعريف متكامل يفيد في تحديد الجرائم الناشئة عن الإنترنت.

النقطة الأولى : موضوع العالم الافتراضي Cyberspace (وبالفرنسية Cyberespace) الذي هو عبارة عن العالم المرئي The virtual world أو المجال الحيوي للبيانات وحركتها المعلوماتية، وهو العالم المختفي في الآلة التقنية[2]. والذي يطلق عليه الفقه العربي تسمية الفضاء الإلكتروني[3]. وهو العالم الذي ابتكر فكرته كاتب الخيال العلمي الشهير William Gibson في روايته الشهيرة The NeuRomancer، التي أصدرها عام 1984، حيث وصف في هذا الكتاب فانتازيا إلكترونية Fantasy Electronic[4] تقابل فيها مجموعة هكرة من مهرة الحاسوب،

(1) د. محمد سامي الشوا، ثورة المعلومات وإنعكاساتها على قانون العقوبات، ص 7 .

(2) RCMP, op-cit.

(3) د. جميل عبد الباقي الصغير، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1999، ص 5 .

(4) (NICHOLSON) Keith – International Computer Crime : A Global Village Under Siege – New England International & Comparative Law Annual 1996 – New England School of Law P. I. available online is Sep. 2001 at :
http://www.nest.edu/annual/vol2/computer.htm

وطالما نشاطهم الاختراق والعديد من المظاهر التي تكاد تصل في بعض الأحيان إلى منطق الجريمة عبر الإنترنت كما هي مقررة في التشريعات المعاصرة.

وإذا كانت الإنترنت لم يتم تعريفها بعد في النظم القانونية المقارنة بشكل مستقل، فإنه مع ذلك قد لجأت تلك النظم - بإيعاز من الفقه - إلى حيلة قانونية يمكن معها الحصول على تعريف قانوني لها، وذلك باستخدام مصطلح منبثق عن عالمها الافتراضي Cyberspace وهذا المصطلح هو CyberLaw أي النظام القانوني للعالم الافتراضي للإنترنت أو قانون الإنترنت وهو "مجموعة القواعد القانونية التي تنظم العالم الفعلي للإنترنت" ، وهي قواعد لم تزل بعد في طور النمو نتيجة لعدم إمكانية حدوث ملاءمة بين المنظومة التقليدية للقانون وبينها، حتى وإن وصفت بالغموض والإبهام.

وإذا كان قانون العالم الافتراضي / الإنترنت (Cyber Law)، لا يشكل عقبة في إطار بناء نظريته - إن أمكن تكاثف الجهود نظريا على الأقل - فإن الحال غير ذلك فيما يتعلق بتطبيق هذه النظرية وتنفيذها سيما في النطاق القضائي. ذلك إن تركيبة قانون العالم الافتراضي/ الإنترنت ذات طبيعة مختلفة في الحقيقة عن تركيبة أي قانون آخر، فهو يتركب من طبيعة افتراضية ذات بعد دولي[1] يتطابق شكليا مع مفاهيم العولمة، وليس مع

(1) TRANSNAIONAL NATURE OF CYBERSPACE, (CYBERCRIME AND CYBERPUNISHMENT< ARCHAIC LAW THERATEN GLOBAL INFORMATION p. 2 report prepared by : McConnell INTERNATIONAL http://www.mcconnellinternational.com with support from WITSA http://www.witsa.com December 2000 availale online in dec. 2000, at: http://www.mcconnellinternational.com/services/cybercrime.html

المفاهيم التي يعرفها القانون الدولي، في الوقت الذي يتسع مدلوله ليشمل فروع القانون الأخرى. ذلك إنه من خلال مصطلح CyberLawهرع الفقه المقارن ليضع تفريعات جدية لهذا المصطلح تعمل في إطاره ووفق فروع القانون المعمول بها، مثل Cyberbehavior للدلالة على سلوكيات القانون المدني، ومصطلح CyberCrime للدلالة على سلوكيات القانون الجنائي، ومصطلح Cybercommerce للدلالة على سلوكيات القانون التجاري، ومصطلح Cyberinvestigation للدلالة على الإجراءات الجنائية في إطار قانون الإنترنت، ومصطلح Cybertribunal على المحاكمات عبر الإنترنت ... إلخ.

هذا الاتجاه الفقهي يسعي إلى إقامة علاقة بين القانون وبين الإنترنت في معني إحداث ملاءمة بين الأثنين، بما يمكن معه تطويع القانون للإنترنت لمصلحة الإنسان في تعامله مع الآلة.

إن عملية إحداث ملاءمة بين النظام القانوني القائم وبين الإنترنت كانت قد برزت بداية حال موافقة الفقه النسبية على إمكانية التعامل القانوني مع الإنترنت بأسلوب التنظيم النفسي للإنترنت Self – regulation ، بحيث يجب ألا يكون هذا التنظيم هو الأداة الوحيدة وإنما يقبل إلى جوار التنظيم القانوني بالأداة التشريعية تواجد أدوات تنظيمية نابعة من طبيعة الإنترنت، أي التقنية المعلوماتية. وسببية رفض وحدة التنظيم الذاتي كنظام قانوني للإنترنت يكمن في أن التنظيم الذاتي ليس مقنعا بالدرجة الكافية[1] بما يجعل العالم الافتراضي آمنا بالدرجة الكافية التي تسمح بالأمن والاستقرار[2]. على

(1) RCMP, op-cit.

(2) CyberCrime And Cyberpunishment , archaic law threatens global information op-cit p. 2

إن الأمر ليس على ذلك القدر من السهولة إذا تأملنا الاتجاه المضاد الذي يأخذ بضرورة التدخل القانوني لتنظيم العالم الافتراضي حيث أنه توجد لديه صعوبات أيضا، من حيث إن أهم صعوبة تتمثل في تحديد طبيعة النظام القانوني الذي يحكم الإنترنت، وهل تكفي النظم الأساسية في الدولة لحسم هذه الصعوبات وتذليل محتواها، أم إن العالم الافتراضي قام هكذا فجأة وبالتالي يمكن أن يوجد له أساس في النظم القانونية المعاصرة، إلا أن العقل القانوني لم يستظهر هذا الأساس بعد، وهنا فإن المسألة فقط تحتاج إلى مزيد من الوقت والتأمل والحكمة القانونية.

النقطة الثانية: ترتبط بالنتائج المترتبة في النظام القانوني حين فصل جرائم الحاسوب Computer Crimes عن جرائم الإنترنت CyberCrime، ومدى إمكانية قيام هذا الفصل تقنيا. والحقيقة إنه من الصعوبة بمكان فصل جرائم الحاسوب عن جرائم الإنترنت، نتيجة لارتباط الإنترنت بالحاسوب ارتباطا تقنيا. إلا أن هذه الصعوبة سوف تتقلص كثيرا إذا أدركنا أن تقنية الحاسوب أعم كثيرا من تقنية الإنترنت. فهو - أي الحاسوب- ثورة حقيقية ذات أبعاد اجتماعية وسياسية واقتصادية وقانونية ليس لها نهاية، إذ كما أنتجت تقنية الحاسوب الإنترنت فإن ذلك لا يعني نهاية المطاف في هذا الشأن، فالمؤشرات السائدة تشير إلى أن تقنيات جديدة للحاسب تبرز في الأفق قريبا , وتدليلا على ذلك فإن دولا كندا تربط جرائم الانترنت بجرائم الاتصال عن بعد Telecommunication Crime التي يمكن أن تقع بواسطة الانترنت كما يمكن إن تقع بواسطة الهاتف وجهاز الموجات الصغيرة Microwave والأقمار الصناعية Satellite وغير ذلك[1].

(1) FGSSC – available online in feb 2000 at :
Http://www.usdoj.gov/criminal/cybercrime/search docs/toc.htm

وإذا كان حقيقي إن تقنية الحاسوب قد انطلقت لكي تبتكر الانترنت فإن منطقه الخلاف بين العمل السلبي الذي يكون محله الحاسوب وبين ذلك الناجم عن استخدام الانترنت يعد أحد الصعوبات الجديدة التي تواجه فقه القانون حقيقة فإذا تحدد هذا التعريف فإنه من السهولة التوصل إلى بحث التوجه السياسي والتشريعي في دولة ما. لأجل ذلك نجد إن البعض لا يمانع في إطلاق صفة جرائم الحاسوب Computer Crime على الاختراق Hacking إلا أنه يشترط بالضرورة أن يكون الحاسوب مرتبطا بشبكة Connected 1 أو Protected Computer ويمكن القول إجمالا إن هناك اتجاهين في إطار رصد تعريف جرائم الانترنت, الاتجاه الأول بنحو منحى التعريف المضيق الذي يقوم برصيد جرائم الانترنت في ربط جرائم العالم الافتراضي ككل بالحاسوب حيث يذهب هذا الاتجاه إلى " إن مصطلح العالم الافتراضي مرجعه استخدام الحاسوب لتسهيل ارتكاب الجرائم 2 وهو تعريف مضيق لكونه يربط إجرام العالم الافتارضى بالحاسوب بالمفهوم الضيق , حيث أن مصطلح الحاسوب يتسع لي أبعد من ذلك الذي نعرفه اليوم وبحيث يجب الأخذ في الاعتبار تلك النظرة المستقبلية للحاسوب التي تعنى حوسبة أو رقمية العالم البشرى على النحو الذي يحقق اعتماد

---

(1) Nicholson – International computer crime op – cit P.2

(2) (KATYAL) Neal Kumar – criminal law in criminal law in Cyberspace , Georgetown University law center 2000< P.13 A revised version of This working paper is forthcoming in the university of Pennsylvania law review < Volume 149 April 2001 This paper can be downloaded without charge from the social science research Network Electronic paper collection at

Http://papers.ssrn.com/ aperitif abstract id=249030 working paper No 249030.

الإنسان عليه في كل شيء لذلك فإن النقد الذي يمكن توجيهه إلى هذا التعريف إنه يربط تعريف جرائم الانترنت بالحاسوب فإن ذلك يعنى أن فصل الحاسوب عن الانترنت في أبسط مظاهر هذا الفصل (أي بفصله بعدم الدخول إلى الانترنت – أو بفضل الكهرباء عنه) يعنى أنتها الجريمة وعدم اتصالها بنا , في حين أنذلك غير صحيح إذ تظل الجريمة قائمة وظاهرة في أماكن أخرى .

لذلك فإن الأرجح هو الاتجاه إلى التوسع في تعريف جرائم العالم الافتارضى/ الانترنت ومكمن التعريف الموسع هو السعي إلى بحث استقلالية لجرائم الانترنت تتنافى مع ربطها بالحاسوب وجرائمه. ولما كنا فيما سبق قد عرفنا الانترنت هي في الحقيقة الجرائم الناشئة عن استعمال هذا التواصل بين الشبكات وهذا اتجاه المشرع الأوروبي في اتفاقية الجريمة عبر العالم الافتراضي المؤرخة 2001/11/23 وكذلك اتجاه المشرع الامريكى حين رصده لمصطلح Protected Computer ولما كان التقسيم الأمثل لهذه الشبكة إلى ثلاثة أقسام كما عرضنا لذلك فيما سلف (شبكة المعلومات الدولية – البريد الإلكترونى- الاتصال المباشر)، فإن العدوان باستخدام الانترنت من خلال أقسامها هو الوضع الصحيح الذي يجب أن يكون عليه التجريم هنا لذلك نجد إن جرائم الانترنت في حقيقتها هي تلك الجرائم التي ترتكب بدواسة التواصل بين الشبكات .

وإذا كان هذا التعريف يتميز بالعمومية إلا أنه مع ذلك يظل محصورا في إطار الانترنت وبالتالي كل جريمة من الجرائم كانت وسيلتها الانترنت أو أقسامها إنما هي من جرائم الانترنت.

إن التعريف الذي نقول به يجعلنا في الحقيقة نعترف مسبقا بأن ظاهرة الانترنت لا زالت غامضة في دراسات القانون وفى هذا الإطار رصد المرشد الفيدرالي الأمريكي لتفتيش وضبط الحاسوب Federal guidelines for searching and computers أهمية الاعتراف بأن رجال القانون بدءوا في مواجهة مشاكل جديدة على اثر إنجاز ثورة معلومات الحاسوب والاتصالات في القرن الواحد والعشرين[1].

إن الفصل بين الحاسوب وبين برمجياته يعد تدليلا على قيمة الفصل بين الحاسوب وبين الانترنت. ولقد اشتد الصراع – بناء على ما سلف – بين فقه القانون وخبراء تكنولوجيا المعلومات خول الأبعاد الفلسفية لتحديد جرائم الانترنت أو جرائم العالم الافتراضي, ما بين مؤيد لاعتبار هذه الجرائم مجرد جرائم عادية ترتكب بواسطة الحاسوب والياته – وهو الأمر الذي يترتب عليه تطبيق القانون السائد عليها وبما لا يخرج عما هو مقرر في هذا الشأن كما أنه يقود إلى القول بكفاية النصوص الجنائية للانطباق عنا لكونها لا تتعدى ما هو مقرر حين اختراق القانون الجنائي كما هو الشأن في الانتهاك Trespass والاختلاس larceny والقرصنة Conspiracy - وبين مؤيد لاعتبار جرائم الانترنت إنما هي جرام ذات أبعاد جديدة وتحتاج إلى إعادة نظر في هيكلة القانون الجنائي الحالية ويدلل هذا الاتجاه على ذلك بموضوعات القانون الجنائي وصعوبة الإثبات وكذلك حالة مرتكبي جرائم أو ما يطلق عليه مشكلة الهكرة Hacklers في هذا الإطار[2] وإذا كان هذا

(1) Theoumyre – abuse in the cyberspace , op-citP.8

(2) Eric J . Sinrod and William P.reilly- Crimes : A practical approach to the application of federal computer crime laws P.3 Santa Clara computer and high technology law Journal may 2000 Volume 16, Number 2.

الاتجاه له منطقة في ضرورة التعامل مع جرائم الانترنت بخصوصية ما إلا أن عملية الكشف عن هذه الخصوصية التي تتمتع بها هذه التوعية من الجرائم استلزم ضرورة التطرق إلى الخصوصية التي تمتع بها الانترنت ذاتها وأما النقطة الثالثة: التي يجب الانطلاق منها للتأكيد على تعريف جرائم الانترنت من منطلق أنها جرائم ترتكب بواسطة تلك الوسيلة أو الأداة التواصلية بين الشبكات دون اعتبار للحدود الدولية, تتعلق بكينونة الانترنت كظاهرة لها ايجابياتها وسلبياتها فإنه يجب معاملتها على هذا الأساس مثلها في ذلك مثل الظواهر الجديدة. لذا فهي ليست مجرد وسيلة لارتكاب الجرائم وذلك لما توفره من مجموعة بدائل مختلفة عبرها , حيث انه يمكن ارتكاب الجرائم بواسطة البريد الالكتروني مثلا (الذي يحتوى على مجموعة بدائل مختلفة) كما يمكن ارتكاب جرائم عبر البدائل التي توفرها شبكة المعلومات الدولية ... الخ

ومن هذا المنطلق فإن الروية المحددة للانترنت لا تنطلق من الفكر النظري وإنما من الواقع العملي , وهذا يستدعى البحث في مدى إمكانية المجتمع للتقبل الفكري لها, فهي مجال حيوي Atmosphere في المجتمع قابل لربط عقليته Mentality بها ففي بعض الدول التي مرت بتجارب واقعة عن الانترنت أمكن لها أن تحدث تفاعلا إيجابيا يتواصل مع قانون الانترنت مقلما حدث في الفيليبين على إثر قيام أحد طلبة الجامعة هناك بابتكار فيروس الحب I love You قامت الدولة بتكثيف جهودها لسن قانون في هذا الشأن سيما بعد التدخل الدولي نتيجة لكون الضرر عبر الحدود

الدولية إلى نطاق عالمي فأصاب أجهزة حاسوب حول العالم[1]. فالعالم الفعلي هو جزء من عالمنا غير منفصل عنه, لذلك فهو ليس بعيدا عن إمكانية إحداث تنظيم قانوني له[2], بل إن الفقه ينادي بكينونة عقلية منفردة للانترنت فعلى مبدؤه عالمية التفكير وإقليمية الحركة[3].



(1) Cyber crime And cyberpubishment , archaic law threatens global information op – Cit P.4

(2) Rcmp op-cit " a computers and telecommunications explode into the next century prosecutors and agents have begun to confront new Kind's explode into the next century prosecutors and agents have begun to confront new Kind's of problems "

(3) Thoumyre – abuse in the cyberspace op-cit P.9 : Think Globally and Act locally

الفصل الثانى
الجريمة المعلوماتية
تعريفها.. أسبابها..خصائصها..تصنيفها

لقد أفرزت ثورة الاتصالات والمعلومات: وسائل جديدة للبشرية تجعل الحياة أفضل من ذي قبل؛ غير أنها فتحت الباب على مصراعيه لظهور صور من السلوك المنحرف اجتماعيا التي لم يكن من الممكن وقوعها في الماضي؛ وتخرج عن دائرة التجريم والعقاب القائمة؛ لأن المشرع لم يتصور حدوثها أصلا .

فمن جهة أولى أتاحت نظم الكمبيوتر (الحاسوب) ظهور صور جديدة من الجرائم لم تكن موجودة في الماضي؛ وذلك مثل سرقة المعلومات والأسرار المودعة في قواعد المعلومات؛ ومن جهة ثانية أتاحت هذه النظم الفرصة لارتكاب الجرائم التقليدية بطرق غير تقليدية ؛ كما هو الشأن بالنسبة لجرائم الغش وإتلاف وإفساد المعلومات المخزنة في قواعد المعلومات.

ومن ثم ينقسم هذا الفصل إلى ثلاثة مباحث، تناول المبحث الأول تعريف الجريمة المعلوماتية، واختص المبحث الثانى بالحديث عن أسباب الجريمة المعلوماتية وخصائصها والمجرم المعلوماتى، وجاء المبحث الثالث مركزا على تصنيـف جـرائم المعلوماتية والإنترنت، وأخيرا عكف المبحث الرابع على قضية انتشار الفيروسات المعلوماتية وأساليب الوقاية منها.



المبحث الأول

تعريف الجريمة المعلوماتية

تعددت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع ذلك إلي الخلاف الذى أثير بشأن تعريف هذه الجريمة ومن قبلها تعريف المعلومة ذاتها, فالجرائم المعلوماتية هي صنف جديد من الجرائم, ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها, لأن الجريمة المعلوماتية هي من الظواهر الحديثة؛ وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات. وقد أحاط بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها ولكن الفقة لم يجتمع علي وضع تعريف محدد لها بل أن البعض ذهب إلى ترجيح عدم وضع هذا التعريف بحجة أن هذا النوع من الإجرام ما هو إلى جريمة تقليدية ترتكب بأسلوب إلكتروني.

وعلى أية حال، فإنه على الرغم من تنامى جهود التصدي لظاهرة الإجرام المعلوماتى إلا أنه لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة المعلوماتية، فقد ذهب جانب من الفقه إلى تناولها بالتعريف على نحو ضيق وجانب أخر عرفها على نحو موسع.

- التعريف الضيق للجريمة المعلوماتية:

ذهب الفقيه (merwe) إلى أن الجريمة المعلوماتية هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلى - أو هو الفعل الاجرامى الذي يستخدم في اقترافة الحاسب الآلى كأداة رئيسية. فيما عرفها الفقية (ros blat) بأنها كل نشاط غير مشروع موجة لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الالى والى تحويل طريقه.

وعرفها كلاوس تايدومان بأنها كافة أشكال السلوك غير المشروع الذي يرتكب باسم الحاسب الآلى.

ويرى البعض أن تعريف كلا من (marwe)و(ros blat) جاءا مقصورين على الاحاطة بأوجة الظاهرة الإجرامية أما تعريف كلاوس تايدومان فيؤخذ عليه أن بالغ في العمومية والاتساع؛ لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع.

ويدخل فى نطاق تعريفات مفهوم الجريمة المعلوماتية الضيقة، تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية، حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسب بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا.

- التعريفات الموسعة لمفهوم الجريمة المعلوماتية:

ذهب الفقيهان (michel&credo) إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته, كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلى بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاتة وأى من مكوناته.

وذهب رأى أخر من الفقة إلى تعريف الجريمة المعلوماتية بأنها عمل أو امتناع يأتيه الإنسان، إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقاب.

ويرى جانب من الفقه من أنصار هذا الاتجاة الموسع بأنها كل سلوك اجرامى يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر.

ويذهب البعض إلى أنة عند وضع تعريف محدد للجريمة المعلوماتية يجب مراعاة عدة اعتبارات مهمة منها:-

1- أن يكون هذا التعريف مقبول ومفهوم على المستوى العالمي.
2- أن يراعى هذا التعريف التطور السريع والمتلاحق في تكنولوجيا المعلومات.
3- أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الاجرامى.
4- أن يفرق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية.

- موقف بعض التشريعات والهيئات الدولية من تعريف الجريمة المعلوماتية:

أشارت الأمم المتحدة في المدونة الصادرة عنها بشأن الجريمة المعلوماتية، إلي الخلاف الواقع بين الخبراء حول ماهية العناصر المكونة لجرائم الكمبيوتر أو حتى المتعلقة بالكمبيوتر ولعل ذلك ما يفسر عدم التوصل إلى تعريف متفق علية دوليا لهذه المصطلحات وإن كان هؤلاء قد اتفقوا ضمنا على وجود ظاهرة تتزايد بمعدلات عالمية لتلك الجرائم.

وإن كان مكتب تقييم التقنية في الولايات المتحدة الأمريكية، قد عرف الجريمة المعلوماتية بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا، فإن قانون الكيان الصهيوني(إسرائيل) رقم 5755لسنة 1995 فى شأن جرائم الحاسب الآلى، قد عرفها بأنها تلك الجرائم التي تشمل العبث ببرامج الكمبيوتر على نحو يعوق استخدامها, أو تحل معلومات غير مصرح بها إلا للأشخاص محددين، وكذلك اختراق الكمبيوتر بغرض ارتكاب جريمة أخرى أو بث فيروس من شأنة التأثير على أدائة.

- المفهوم القانوني للمعلومات:

تعتبر المعلومات في الوقت الراهن سلعة تباع وتشترى ومصدر قوة اقتصادية وسياسية وعسكرية، وذلك لارتباطها بمختلف مجالات النشاط الإنساني وتداخلها في كافة جوانب الحياة العصرية, وبات الوعي بأهميتها مظهرا لتقدم الأمم والشعوب.

وسوف نعرض هنا لماهية المعلومة من حيث تعريفها ثم أنواعها والشروط اللازم توافرها فيها، وطبيعتها القانونية, والمسؤلية عنها.

- تعريف المعلومة:

لم تعد المعلومات الآن مجرد نوع من الرفاهية والترف تتباهى به الشعوب أو المنظمات وإنما أصبحت ركيزة أساسية في تقدم وتطور المجتمع وتحقيق تقدمة ورفها يته المنشودة ,وفى سبيل ذلك وضع عدد غير قليل من التشريعات الوطنية المختلفة تعريفا للمعلومة وهوماسوف نعرض للعدد منها.

وقد عرف المشرع الامريكى، المعلومات في قانون المعاملات التجارية الإلكتروني لعام 1999بالفقرة العاشرة من المادة الثانية بأنها تشمل (البيانات والكلمات والصور والأصوات والوسائل وبرامج الكمبيوتر والبرامج المضغوطة والموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابة ذلك.

والتعريف السابق نجد انه قد وسع من مفهوم المعلومة ووضع تقريبا كل ما يتعلق بها بل أكثر من ذلك أنة تحسب ما قد يظهر من تتطور تكنولوجي جديد.

والمشرع الفرنسي ووفقا للقانون 82-652 الصادر في 26 يوليو لسنة 1982، تعرف المعلومة على أنها صورة أو مستندات أو معطيات أو خطابات أيا كانت طبيعتها.

أما قانون البحرين رقم 83 لسنة 2002بشأن المعاملات الإلكترونية فقد عرف المعلومات بأنها (البيانات والنصوص والصور والأصوات والرموز وبرامج الحاسوب والبرمجيات ويمكن أن تكون قواعد البيانات والكلام)

كما عرف قانون إمارة دبي بشأن المعاملات والتجارة الإلكترونية رقم 2 لسنة 2002، المعلومات الإلكترونية بأنها(معلومات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب إلى أو غيرها من قواعد البيانات).

هذه مجموعة من التشريعات التي وضعت تعريفا واضح للمعلومة والمعلومات كان أغلبها كما رأينا يدور حول الأشكال المختلفة للمعلومات وصورها التي تظهر فبها سواء تعلق الأمر برموز أو صور أو بيانات الخ.

وقد ذهب البعض إلى ضرورة التفرقة بين المعلومات والبيانات, فالبيانات تعبر عن مجموعة من الأرقام والرموز والحقائق التي لا علاقة بين بعضها البعض أما المعلومات فهي المعنى الذي يستخلص من هذة البيانات.

- أنواع المعلومات:

تقسم المعلومات إلي ثلاث طوائف هي، المعلومات الاسمية والمعلومات المتعلقة بالمصنفات الفكرية والمعلومات المباحة.

أما الطائفة الأولي وهى المعلومات الاسمية، فتتقسم إلي مجموعتين هما:

1- المعلومات الموضوعية وهى تلك المعلومات المرتبطة بشخص المخاطب بها مثل اسمه وموطنه وحالتة الاجتماعية وهى معلومات لا يجوز الإطلاع عليها إلا بموافقة الشخص نفسه.

2- المعلومات الشخصية ويقصد بها تلك المعلومات المنسوبة آخر مما يستدعى إدلاء الغير برأيه الشخصي فيها وهى مثل المقالات الصحفية والملفات الإدارية للعاملين لدى جه معينه.

وأما الطائفة الثانية، وهى المعلومات الخاصة بالمصنفات الفكرية، فهذه المصنفات محمية بموجب قوانين الملكية الفكري مثل الاختراعات والابتكارات المختلفة والتسجيلات الفنية والمؤلفات الأدبية.

وأما الطائفة الثالثة وهى المعلومات المباحة، فيقصد بها تلك المعلومات تكون مباحة للجميع الحصول عليها لأنها بدون مالك مثل تقارير البورصة والنشرات الجوية هذة المعلومات مباحة للكافة وغير محمية بأي من وسائل الحماية.

- الشروط التي يجب توافرها في المعلومة محل الحماية:

بصفة عامة هناك شروط يجب توافرها في المعلومة حتى تتمتع بالحماية القانونية وتتمثل هذة الشروط في الآتى:

أولا: أن يتوافر فى المعلومة التحديد والابتكار

المعلومة التي تفتقد لصفة التحديد لا يمكن أن تكون معلومة حقيقية فإذا كانت المعلومة هي تعبير وصياغة محددة تجعل رسالة ما قابلة للتبليغ عن طريق علامات أو إشارات معينة

وهذا يتطلب أن تكون محدده تحديدا دقيقا وخصوصا في مجال الاعتداء على الأموال فهذة الاعتداءات تتطلب أن يكون هناك شيء محددا ومبتكر أما الشيء الشائع فلا يتمتع بأي حماية قانونية.

ثانيا : أن يتوافر في المعلومة السرية والاستئثار

السرية صفة لازمة للمعلومة محل الحماية القانونية ,ولا يتصور في جرائم مثل جرائم السرقة والنصب وخيانة الأمانة إذا انعدم هذا الحصر وذلك لان المعلومة العا مة الشائعة تكون بمنأى عن أي حيازة وتكتسب المعلومة وصفها إما بالنظر إلى طبيعتها أو بالنظر إلا إرادة الشخص أو إلي الأمرين معا مثل الرقم السري(passwoard).

إذن حتى تتمتع المعلومة بالحماية القانونية، فلابد أن يتوافر فيها الشرطان السابقان, فإذا فقدتهما أصبحت معلومة غير محمية ولا يملكها أحد وغير قابلة لأن يستأثر بها أي شخص بل أصبحت عامة لكل من يريد استخدامها.



المبحث الثانى
الجريمة المعلوماتية أسبابها .. خصائصها..
المجرم المعلوماتى

لاشك أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الأفعال الإجرامية التقليدية، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع في ارتكاب الفعل غير المشروع[1]، فضلا عن ذلك، تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التى تختلف تماما عن الخصائص التى تتمتع بها الجرائم التقليدية، كما أن الجانى الالكترونى(أو المجرم الالكترونى) يختلف أيضا عن المجرم العادى.

ويأتي في مقدمة أسباب الجريمة المعلوماتية، غاية التعلم والتي تتمثل في استخدام الكمبيوتر والإمكانيات المستحدثة لنظم المعلومات وهناك أمل الربح وروح الكسب التي كثيرا ما تدفع إلى التعدي على نظم المعلومات بالإضافة

(1) وتتنوع الجرائم المعلوماتية على النحو التالي :
- إساءة استخدام الإنترنت.
- استخدام برامج حل وكشف كلمات المرور.
- نشر برامج حصان طروادة وغيرها من الفيروسات.
- هجمات المخربين.
- الهجمات الاختراقية.
- الانتهاكات الأمنية التي تتضمن حالات إساءة استخدام عن طريق الدخول غير المخول به على النظام : تنبع غالبية الانتهاكات الأمنية من مصادر داخلية، مثال : مستخدمين من داخل المؤسسة يحاولون الوصول إلى بيانات سرية غير مخول لهم بالإطلاع عليها.

راجع في ذلك :

Dr. Linda volonino.cyber terrorism. Op. cit.

إلى الدوافع الشخصية والمؤثرات الخارجية التي قد تكون سببا في ارتكاب الجريمة المعلوماتية.

- غاية التعلـــم :

يشير الأستاذ ليفي مؤلف كتاب قراصنة الأنظمة HACKERS إلى أخلاقيات هؤلاء القراصنة والتي ترتكز على مبدأين أساسيين :

1- أن الدخول إلى أنظمة الكمبيوتر يمكن أن يعلمك كيف يسير العالم.

2- أن جمع المعلومات يجب أن تكون غير خاضعة للقيود.

وبناء على هذين المبدأين فإن أجهزة الكمبيوتر المعنية ما هي إلا آلات للبحث، والمعلومات بدورها ما هي إلا برامج وأنظمة معلومات.

ومن وجهة نظر هؤلاء القراصنة فإن جميع المعلومات المفيدة بوجه عام يجب أن تكون غير خاضعة للقيود وبعبارة أخرى أن تتاح حرية نسخها وجعلها تتناسب مع استخدامات الأشخاص.

ويري هؤلاء القراصنة إغلاق بعض نظم المعلومات وعدم السماح بالوصول إلى بعض المعلومات وخاصة بعض المعلومات السرية التي تخص الأفراد.

ويعلق قراصنة الأنظمة أنهم يرغبون في الوصول إلى مصادر المعلومات والحاسبات الإلكترونية والشبكات بغرض التعلم.

وقد لاحظ كل من "ليفي" و "لاندريس" أن قراصنة الأنظمة لديهم الاهتمام الشديد بأجهزة الكمبيوتر وبالتعلم ويدخل العديد منهم في أجهزة الكمبيوتر على أنهم محترفين ويختار بعض القراصنة الأنظمة لتعلم المزيد عن كيفية عمل الأنظمة.

ويقول "لانديس" أن هؤلاء القراصنة يرغبون في البقاء مجهولين حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة لأطول وق ممكن. ويكرس

البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة حيث تتفاوت معرفتهم عن الأنظمة والبرمجة إلى حد بعيد.

وكتب أحد قراصنة الأنظمة يقول : يكتشف قراصنة الأنظمة نقطة ضعف أمنية فيحاولون استغلالها لأنها موجودة بهدف عدم تخريب المعلومات أو سرقتها، أعتقد أن نقوم به يشبه قيام شخص باستكشاف أساليب جديدة للحصول على المعلومات من المكتبة فيصبح في غاية الإثارة والانهماك.

وينبغي ألا نستهين بكفاءة الشبكات التي يتعلم من خلالها القراصنة حرفتهم.

وهم يقومون بالفعل بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم البعض. حيث ذكر أن قراصنة الأنظمة أنه ينتمي إلى مجموعة بحث مهمتها استخراج كميات كبيرة من المعلومات وتعلم أكبر قدر منها.

ويسعي أعضاء القراصنة إلى التخصص والتعاون في المشاريع البحثية وتقاسم البرامج والأخبار وكتابة المقالات وتعريف الآخرين بمجالات اختصاصهم ويدع قراصنة الأنظمة نظاما خاصا لمجال المعرفة الذي يجذبهم ويعلهم التفكير ويسمح لهم بتطبيق ما تعلموه في أنشطة هادفة وإن لم تكن قانونية دائمة[1].

- السعي إلى الربح

أشارت إحدى المجلات المتخصصة في الأمن المعلوماتي securite informatique إلى الرغبة في تحقيق الثراء من بين العوامل الأساسية لارتكاب الجريمة المعلوماتية حيث أشارت :

- أن 43% من حالات الغش المعلن عنها قد بوشرت من أجل اختلاس الأموال.

(1) قراصنة أنظمة الكمبيوتر إعداد : دورثي إي. ديننغ ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ترجمة : آمنة علي يوسف، ديسمبر 1998، ص 8.

- 23% من أجل سرقة المعلومات.
- 19% أفعال اتلاف.
- 15% سرقة وقت الآلة vol detemps machine أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية[1].

لذا نجد أن الدافع لارتكاب الجريمة المعلوماتية يمكن أن تكون سببه مجرد سداد الديون المستحقة أو مشاكل عائلية راجعة للنقود أو ادمان ألعاب القمار أو المخدرات لذا فإن بيع المعلومات المختلسة هو نشاط متسع للغاية ويمكن أن نبين في هذا المجال واقعة استيلاء مبرمج يعمل لدي إحدى الشركات الألمانية على 22 شريطا ممغنطا تحوي معلومات هامة بخصوص عملاء وإنتاج هذه الشركة حيث هدد السارق ببيعها للشركات المنافسة ما لم تدفع له فدية مقدارها 200.000 دولار.

وبعد أن قامت الشركة بتحليل الموقف وقدرت أن الخسائر التي يمكن أن تنشأ عن إفشاء محتواها تفوق بكثير المطلب المطلوب فقد فضلت دفع المبلغ من أجل استرداد الشرائط المسروقة[2].

كذلك أيضا دفعت الرغبة بمستخدم يعمل بشركة التأمين كي يحتفظ بوظيفته التي سبق وأن فصل منها إلى احتجاز الذاكرة المركزية الخاصة بالشركة كرهينة لديه، حيث هدد المختلس رئيسه في العمل بأنه إذا حاول أن يلغي بطاقة أجرته من ذاكرة الحاسب الآلي فإن هذه الأخيرة سوف تدمر تلقائيا عن طريق ما يعرف بالقنابل المنطقية[3].

(1) G. Delmare, securité informatique Ressource informatique no. 1. Juill 1984.

(2) Le Monde informatique 21 fev 1983, Etude la delinquance en col blanc se parte bien

(3) Les escrocs a l'informatique in le Nouvel Economiste no. 202 du 1-10-1979.

- الإثارة والمتعة والتحدي :

يدرك القراصنة : شيئا عن أساسيات الكمبيوتر وأن هذا الأمر يمكن أن يكون ممتعا، حيث جاء على لسان أحد القراصنة ما يأتي كانت القرصنة هي النداء الأخير الذي يبعثه دماغي فقد كنت أعود إلى البيت بعد يوم ممل آخر في المدرسة، وأدير تشغيل جهاز الكمبيوتر، وأصبح عضوا في نخبة قراصنة الأنظمة، كان الأمر مختلفا برمته حيث لا وجود لعطف الكبار وحيث الحكم هو موهبتك فقط. في البدء كنت أسجل أسمي في لوحة النشرات **Bulletin Borard** الخاصة حيث يقوم الأشخاص الآخرين الذين يفعلون مثلي بالتردد على هذا الموقع، ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد.

وبعد ذلك أبدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدأ عقلي بقطع مليون ميل في الساعة وأنسي جسدي تماما بينما أتنقل من جهاز كمبيوتر إلى آخر محاولا العثور على سبيل للوصول إلى هدفي. لقد كان الأمر يشبه سرعة العمل في متاهة إلى جانب الاكتشاف الكبير لإعداد ضخمة من المعلومات.

وكان يرافق تزايد سرعة الأدرينالين الإثارة المحظورة بفعل شيء غير قانوني. وكل خطوة أخطوها كان يمكن أن تسقطني بيد السلطات. كنت على حافة التكنولوجيا واكتشاف ما وراءها، واكتشاف الكهوف الإلكترونية الي لم يكن من المفترض وجودي بها[1].

(1) قراصنة أنظمة الكمبيوتر، إعداد: دروثي إي. ديننغ، ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن، ترجمة: آمنة علي يوسف، ديسمبر 1998 ص 11.

وذكرت Jutian Dibbell بأنها تعتقد بأن المتعة تكمن في المخاطر التي ترتبط بعملية القرصنة وذكرت قائلة "أن التكنولوجيا تستسلم من الدراما المليئة بالمغامرات وأن قراصنة الأنظمة يعيشون في عالم لا يعتبرون فيه العمل السري سوي لعبة يلو بها الأطفال.

- الدوافع الشخصية :

إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميل مرتكبوا جرائم نظم المعلومات إلى إظهار تفوقهم ومستوي ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبوا هذه الجرائم لديهم شغف الآلة يحاولون إيجاد – وغالبا ما يجدون – الوسيلة إلى تحطيمها بل والتفوق عليها[1].

ويتزايد شيوع هذا الدافع لدي فئات صغار السن من مرتكبي الكمبيور الذين يمضون وقتا طويلا أما حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الكمبيوتر وشبكات المعلومات وإظهار تفوقهم على وسائل التكنولوجيا، الأمر الذي دفع بالعديد من الفقهاء إلى المناداة بعدم مساءلة مرتكبي جرائم الحاسب الآلي الذي يتمثل باعثهم في إظهار تفوقهم، واعتبار أعمالهم غير منطوية على نوايا آثمة.

(1) يميل القراصنة إلى التحدي وإلى معرفة تفاصيل تكنولوجيا الكمبيوتر ويبدو أن ولعهم بالكمبيوتر يدفعهم إلى ارتكاب الجرائم وفي هذا الخصوص يحدثنا الدكتورPerey Black أستاذ علم النفس بجامعة نيويورك أن القراصنة يتملكهم جميعا شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الكمبيوتر إلى تعويضهم عن الإحساس بالدونية.

راجع في ذلك :

CYBER CRIME op. cit. p. 25.

وقد أمكن الكشف في بعض الأحوال عن أن مجرد إظهار شعور جنون العظمة وهو الدافع لارتكاب فعل الجريمة المعلوماتية وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي وهو مفتاح سر كل نظام قد ينتابه إحساس بالإهمال أو بالنقص داخل المنشأة التي يعمل بها[1]. وقد يندفع تحت تأثير الرغبة القوية من أجل تأكيد قدراته الفنية لإدارة المنشأة إلى ارتكاب الجريمة المعلوماتية، ومن ثم يجد ترضية من خلال الإفصاح عن شخصيه أمام العامة[2].

- ضحايا جريمة سرقة المعلومات :

تتميز جرائم الحاسب بالصعوبات البالغة في اكتشافها وبالعجز في حالات كثيرة عن إمكان إثباتها في حالة إكتشافها.

ومرد ذلك الأسباب التالية :

أولا : لا تخلف جرائم الحاسب آثارا ظاهرة خارجية فهي تنصب على البيانات والمعلومات المختزنة في نظم المعلومات والبرامج مما ينفي وجود أي أثر مادي يمكن الاستعانة به في إثباتها، فالجرائم المعلوماتية ينتفي فيها العنف وسفك الدماء ولا توجد فيها آثار لاقتحام سرقة الأموال، وإنما هي أرقام ودلالات تتغير أو تمحي من السجلات ومما يزيد من هذه الصعوبة ارتكابها في الخفاء، وعدم وجود أثر كتابي مما يجري من خلال تنفيذها من عمليات حيث يتم نقل المعلومات بواسطة النبضات الإلكترونية.

(1) تمت مقاضاة شركة مورجان ستانلي مر تبين من قبل الموظفين العاملين بها بسبب التمييز العنصري حيث كشفت مبادئ الطب الشرعي المستخدمة في مجال جرائم الكمبيوتر عن وجود "نكات عنصرية" يتم توزيعها عبر نظام البريد الإلكتروني الخاص بالشركة.
راجع في ذلك :

DR Linda Volonino op.cit.

(2) د. محمد سامي الشواء سابق الإشارة إليه، ص ص 52-53 .

ثانيا : يتم ارتكاب جريمة الحاسب عادة عن بعد فلا يتواجد الفاعل في مسرح الجريمة حيث تتباعد المسافات بين الفاعل والنتيجة، وهذه المسافات لا تقف عند حدود الدولة بل تمتد إلى النطاق الإقليمي لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها.

ثالثا : تبدو أكثر المشاكل جسامة لا في مجال صعوبة اكتشاف وإثبات جرائم الحاسب بل وفي دراسة هذه الظاهرة في مجملها هي مشكلة امتناع المجني عليهم عن التبليغ عن الجرائم المرتكبة ضد نظام الحاسب وهو ما يعرف بالرقم الأسود **chiffrenoir**(1) حيث لا يعلم ضحايا هذه الجرائم شيئا عنها إلا عندما تكون أنظمتهم المعلوماتية هدفا لفعل الغش أو حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل(2).

خصائص الجرائم المتصلة بالكمبيوتر والمعلوماتية:

تتميز الجرائم المرتكبة بواسطة الكمبيوتر كأداة أو كهدف للجريمة بالخصائص التالية:

1- سرعة التنفيذ: لا يتطلب تنفيذ الجريمة عبر الهاتف الوقت الكبير،

---

(1) Dr. Francillon, Les crimes inormatiques et d'autres crimes dans le domaine de la technologie informatique en france Rev. int. pén, 1990, vol 64, p. 293

(2) في إحدى الوقائع الشهيرة تعرض بنك merchant bank city في بريطانيا لنقل 8 مليون جنيه من أحد أرصدته إلى رقم حساب في سويسرا، وقد تم القبض على الفاعل أثناء محاولته سحب المبلغ المذكور ولكن البنك يدل الادعاء على الفاعل قام بدفع مبلغ مليون جنيه له بشرط عدم إعلام الآخرين عن جريمته وشريطة إعلام البنك عن الآلية التي نجح من خلالها باختراق نظام الأمن الخاص بحاسوب البنك الرئيسي.
راجع في ذلك : يونس خالد عرب مصطفي، جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير مقدمة إلى الجامعة الأردنية 1994، ص 72.

وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر. وهذا لا يعني إنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

2- التنفيذ عن بعد: لا تتطلب جرائم الكمبيوتر في أغلبها (إلا جرائم سرقة معدات الكمبيوتر) وجود الفاعل في مكان الجريمة.بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل سواء كان من خلال الدخول للشبكة المعنية أو اعترض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب...الخ.

3- إخفاء الجريمة: أن الجرائم التي تقع على الكمبيوتر أو بواسطته كجرائم (الإنترنت) جرائم مخفية، إلا انه يمكن أن تلاحظ آثارها، والتخمين بوقوعها.

4- الجاذبية: نظرا لما تمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الأجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويلا مسارها أو استخدام أرقام البطاقات...الخ.

5- عابرة للدول: إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، وأصبحت ساحتها العالم أجمع.

ففي مجتمع المعلومات تذوب الحدود الجغرافية بين الدول، لارتباط العالم بشبكة واحدة، حيث أن أغلب الجرائم المرتكبة عبر شبكة الإنترنت، يكون الجاني فيها في دولة ما والمجني عليه في دولة أخرى،وقد يكون الضرر المترتب عن الجريمة ليس واقعا على المجني عليه داخل إقليم دولة

الجاني، وتعارض المواد المعروضة مع الثقافات المتلقية لها خاصة إذا كانت تتعارض في الدين والعرف والاجتماعي والنظام الأخلاقي والسياسي للدولة.

6- جرائم ناعمة: تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح.إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفا،فنقل بيانات من كمبيوتر إلى أخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن.

7- صعوبة إثباتها: تتميز جرائم الإنترنت عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي(بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة.

8- التلوث الثقافي: لا يتوقف تأثير الجرائم المتصلة بالكمبيوتر عند الأثر المادي الناجم عنها وإنما يتعدى ذلك ليهدد نظام القيم والنظام الأخلاقي خاصة في المجتمعات المحافظة والمغلقة.

9- عالمية الجريمة والنظام العدلي: نظرا لارتباط المجتمع الدولي إلكترونيا،فقد أصبح مجتمعنا تخيليا مما أدى إلى أن تكون ساحة المجتمع الدولي بكافة دوله ومجتمعاته مكانا لارتكاب الجريمة من كل مكان ، مما أن تطلب أن تمارس الدول المتطورة وخاصة الصناعية على الدول النامية من أجل سن تشريعات جديدة لمكافحة الجرائم المتصلة بالكمبيوتر مما استدعى أن تكون القوانين ذات صبغة عالمية.

10- لا يتم - في الغالب الأعم - الإبلاغ عن جرائم الانترنت: إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير. لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالمصادفة؛ بل وبعد وقت طويل من ارتكابها، زد على

ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها. فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة؛ والعدد الذي تم اكتشافه؛ هو رقم خطير. فالفجوة بين عدد هذه الجرائم الحقيقي؛ وما تم اكتشافه: فجوة كبيرة.

11- من الناحية النظرية: يسهل ارتكاب الجريمة ذات الطابع التقني؛ كما أنه من السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها.

12- لذا فهذه الجرائم لا تترك أثرا لها بعد ارتكابها: علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت . فهذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم جرائم الانترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها.

13- تعتمد هذه الجرائم على قمة الذكاء في ارتكابها؛ ويصعب على المحقق التقليدي التعامل مع هذه الجرائم. إذ يصعب عليه متابعة جرائم الانترنت والكشف عنها وإقامة الدليل عليها. فهي جرائم تتسم بالغموض؛ وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية.

14- الوصول للحقيقة: بشأنها تستوجب الاستعانة بخبرة فنية عالية المستوى.

15- عولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي: لتعقب مثل هذه الجرائم؛ فهذه الجرائم هي صورة صادقة من صور العولمة؛ فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد وقد يتعدد هذا المكان بين أكثر من دولة؛ ومن الناحية الزمنية تختلف المواقيت بين الدول؛ الأمر الذي يثير التساؤل حول: تحديد القانون الواجب التطبيق على هذه الجريمة.

16- صعوبة المطالبة بالتعويض المدني بخصوص جرائم الانترنت.

المجرم المعلوماتى:

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره في تمييز المجرم المعلوماتى عن غيره من المجرمين العاديين الذين جنحوا إلى السلوك الاجرامى النمطي. وهذا ماسو ف نعرض له موضحين أهم سمات المجرم المعلوماتى ثم خصائصة المميزة وأخيرا لأنماط هذا المجرم وذلك على النحو التالي.

- سمات المجرم المعلوماتي:

يمكن أن نستخلص مجموعة من السمات التي يتميز بها المجرم المعلوماتى، والتي يساعد التعرف عليها مواجهة هذا النمط الجديد من المجرمين، ويعد الأستاذ (parker) واحد من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامه والمجرم المعلوماتى بصفة خاصة، ويرى (parker) أن المجرم المعلوماتى وإن كان يتميز ببعض السمات الخاصة إلا انه في النهاية لا يخرج عن كونة مرتكبا لفعل إجرامى يتطلب توقيع العقاب علية.

وفيما يلى عرضا لبعض السمات العديدة للمجرم المعلوماتى والتي في الغالب تميزه عن غيره من المجرمين العاديين:

أولا: المجرم المعلوماتى، مجرم متخصص

تبين في عديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يعكس أن المجرم الذي يرتكب إلا جرام المعلوماتى هو مجرم في الغالب متخصص في هذا النوع من الإجرام.

ثانيا: المجرم المعلوماتى، مجرم عائد إلى الإجرام

يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وأدت إلى تقديمهم إلى المحاكمة في المرة السابقة، ويودى ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلى تقديمهم إلى المحاكمة.

ثالثا: المجرم المعلوماتى، مجرم محترف

يتمتع المجرم المعلوماتى باحترافية كبيرة في تنفيذ جرائمة، حيث أنه يرتكب هذة الجرائم عن طريق الكمبيوتر الأمر يقتضى الكثير من الدقة والتخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية.

رابعا: المجرم المعلوماتى، مجرم غير عنيف

المجرم المعلوماتى من المجرمين الذين لا يلجأون إلى العنف بتاتا في تنفيذ جرائمهم وذلك لأنه ينتمي إلى إجرام – الحيلة – فهو لا يلجا إلى العنف في ارتكاب جرائمة، وهذا النوع من الجرائم لا يستلزم أي قدرا من العناء للقيام به.

فضلا عما تقدم، فالمجرم المعلوماتى مجرم ذكى، ويتمتع بالتكيف الاجتماعي، أي لا يناصب أحد العداء وأيضا يتمتع بالمهارة والمعرفة وأحيانا كثيرة على درجة عالية من الثقافة.

- خصائص المجرم المعلوماتى:

يتميز المجرم المعلوماتى كذلك بمجموعة من الخصائص التي تميزة بصفة عامة عن غيرة من المجرمين، وهى:

أولا: المهارة

يتطلب تنفيذ الجريمة المعلوماتية قدرا من المهارة يتمتع بها الفاعل، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال التكنولوجي، أو بمجرد التفاعل الاجتماعي مع الآخرين، وهذة ليست قاعدة في أن يكون المجرم المعلوماتى على هذا القدر من العلم ,وهذا ما اثبتة الواقع العملي أن جانب من انجح مجرمي المعلوماتية، لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الإجرام.

ثانيا: المعرفة

تميز المعرفة مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتى أن يكون تصورا كاملا لجريمته، ويرجع ذلك إلى أن المصرح الذي تمارس فية الجريمة المعلوماتية هو نظام الحاسب الأولى, فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة وذلك قبل تنفيذ الجريمة

ثالثا: الوسيلة

ويراد بها الإمكانيات التي يحتاجها المجرم المعلوماتى لإتمام جريمتة. وهذه الوسائل قد تكون في غالب الأحيان، وسائل بسيطة وسهلة الحصول عليها خصوصا إذا كان النظام الذي يعمل بة الكمبيوتر من الأنظمة الشائعة أما إذا كان النظام من الأنظمة غير المألوفة، فتكون هذة الوسائل معقدة وعلى قدر من الصعوبة.

رابعا: السلطة

يقصد بالسلطة، الحقوق والمزايا التي يتمتع بها المجرم المعلوماتى والتي تمكنة من ارتكاب جريمتة، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة.

وقد تتمثل هذة السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوى على المعلومات وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الالى وإجراء المعاملات، كما أن السلطة قد تكون شرعية من الممكن أن تكون غير شرعية كما في حالة سرقة شفرة الدخول الخاصة بشخص آخر.

خامسا: الباعث

وهو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة ويضل هو الباعث الأول وراء ارتكاب الجريمة المعلوماتية ،. ويرى البعض أيضا ما يخالف ذلك في أن الربح المادي لا يعد هو الباعث في أغلب الأحيان على ارتكاب جرائم المعلوماتية وإنما هناك أمور عديدة أخرى

في الغالب تكون هي الباعث مثل الانتقام من رب العمل، وأيضا مجرد الرغبة قهر نظام الحاسب واخترا ق حاجزة الامنى.

- الأنماط المختلفة للمجرم المعلوماتى:

يقسم مجرمي المعلوماتية (cybr criminals) إلي مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال إلي وجود عدد من الأنماط المختلفة لمجرمي المعلومات، نرصدها فيما يلى:

الطائفة الأولي(**pranksters**):

وهم الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين دون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم. ومن أمثلة هذة الطائفة صغار مجرمي المعلوماتية.

الطائفة الثانية(**hackers**):

وتضم الأشخاص الذين يستهدفوا من الدخول إلى أنظمة الحاسبات الآلية الغير مصرح لهم بالدخول إليها كسر الحواجز الأمنية الموضوعة لهذا

الغرض وذلك بهدف اكتساب الخبرة وبدافع الفضول، أو لمجرد إثبات القدرة على اختراق هذة الأنظمة.

الطائفة الثالثة(**malicious hackers**):

وهم أشخاص هدفهم إلحاق خسائر بالمجني عليهم، دون أن يكون الحصول على مكاسب مالية ضمن هذة الأهداف، ويندرج تحت هذة الطائفة الكثير من مخترعي فيروسات الحاسبات الآلية وموزعيها.

الطائفة الرابعة(**personal problem solvers**):

وهم الطائفة الأكثر شيوعا من مجرمي المعلوماتية فهم يقومون بارتكاب جرائم المعلوماتية بحيث يترتب عليها في كثير من الأحيان خسائر كبيرة تلحق بالمجني عليه، ويكون الباعث في هذة الجريمة إيجاد حلول لمشاكل مادية تواجة الجاني
لا يستطيع حلها بالطرق العادية.

الطائفة الخامسة(**career criminals**):

وهم مجرمي المعلوماتية الذين يهدفون من وراء نشاطهم الاجرامى تحقيق ربح مادي بطريق غير مشروع، ويقترب المجرم المعلوماتى من هذة الطائفة في سماتة إلى المجرم التقليدي.

ومن جانب آخر، أكدت بعض الدراسات والأبحاث العلمية على أن فئات المجرمين(أو الجناة) تنحدر من:

1- مستخدمو الحاسب بالمنازل.
2- الموظفون الساخطون على منظماتهم.
3- المتسللون ومنهم الهواة أو العابثون بقصد التسلية.
4- المحترفون الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يسرقون محتوياته وتقع أغلب جرائم الانترنت حاليا تحت هذه الفئة بتقسيمها.

5- العاملون في الجريمة المنظمة .

ويتمتع هؤلاء الجناة بصفات أخرى غير متوفرة فى الجناة العاديين نذكر منها:

1- أعمارهم تتراوح عادة بين 18 إلى 46 سنة والمتوسط العمري لهم 25 عاما .
2- المعرفة والقدرة الفنية الهائلة .
3- الحرص الشديد وخشية الضبط وافتضاح الأمر .
4- ارتفاع مستوى الذكاء ومحاولة التخفي .

ومن الجدير بالذكر فى هذا الصدد أن هناك اتفاق بين الخبراء والمتخصصين على أن جرائم الانترنت تمثل تحديا جديدا في عالم الجريمة، وذلك للأسباب التالية:

- صعوبة التعرف على هوية الجاني:

فهو لا يترك أثرا لجريمته، وان وجد فقد لا تدل عليه.

- وجود بعض العقبات في محاكمة الجاني:

حال اكتشاف هويته إذا كان من بلد لا يعتبر ما قام به جرما.

- اتساع شريحة الجناة لتشمل صغار مستخدمي الانترنت:

بسبب توفر الوسائل والبرامج المستخدمة في التخريب لصغار مستخدمي الانترنت، مما يجعل جرائم الانترنت لا تتطلب خبرة عالية.

- نقص الوعي بسلبية الاستخدام السيئ للانترنت:

مما يجعل البعض ينظر للأعمال التخريبية على الانترنت – كاختراق المواقع – عمل بطولى.



المبحث الثالث

تصنيـف جــرائم المعلوماتية والإنترنت

أولا: الجرائم المرتكبة أثناء أداء الحاسب لوظائفه العادية

لا يتطلب ارتكاب هذا النوع من الجرائم المساس بالوظائف العادية للحاسب الآلي ولا تعديل على البيانات المختزنة بذاكرته بل يقتصر الأمر على الدخول من جانب البعض إلى مركز نظم المعلومات وأداة إلكترونية تسمح بالتقاط المعلومات أو التنصت عليها من بعد.

ثانيا: الاختراق وانتحال الهوية

من الممكن الاختراق أو انتحال الهوية إما ماديا أو إلكترونيا. فالاختراق المادي يسمح بالدخول في مناطق خاضعة للسيطرة عن طريق بوابات إلكترونية أو آلية. وأسلوب الاختراق الأكثر شيوعا هو أن يقف شخص غير مسموح له بالدخول أمام البوابة المغلقة حاملا بين ذراعية متعلقات خاصة بالحاسب الآلي كالشرائط الممغنطة desbandes أو ينتظر حتى يتقدم شخص مسموح له بالدخول ويفتح له الباب فيدخل معه في نفس الوقت. لذا فإنه يمكن القول بأن التواجد في صالات الحاسبات الآلية هو أمر حتمي لارتكاب هذه الجرائم[1]. وينطوى الفعل غير المشروع هنا على اطلاع غير مسموح به على المعلومات المختزنة في نظم المعلومات وله صور عديدة.

1- سرقة القائمة وهي عملية مادية بحتة يكتفي فيها السارق بسحب القائمة من الطابعة.
2- الإطلاع على المعلومات والمقصود بذلك مطالعة المعلومات التي تظهر على شاشة الحاسب الآلي.

(1) انظر :

D. Parker, op. cit., p. 44 et s.

3- التصنت المجرد على المعلومات ويتم ذلك عن طريق استخدام مكبر للصوت[1] والذي يلتقط المعلومات والبيانات.

(1) قبل أن يقوم Hacker باقتحام شبكة الحاسب الآلي، يجب عليه استخدام تسهيلات اتصال لكي يرتبط بالشبكة وقد يكون تكاليف الاتصال القانوني مع نظام الكمبيوتر المستهدف معرفة الـ Hackers قد تكون مرتفعة للغاية وقد يكون من الممكن تعقبها. لذا يقوم الـ Hackers بتوظيف أساليب فنية لتجنب هاتين= =المشكلتين: يقوم الـ Hackers بتوظيف أساليب فينة يطلق عليها عادة الـ Phreaking ومن تطبيقاتها ما يلي :

-1 الاتصال التليفوني بواسطة النغمة : وهو أسلوب نقلي يمكن التلاعب من خلاله في شبكات الاتصالات عن طريق استعمال تردد النغمات، أن النغمات يمكن استعمالها لتنشيط وتفعيل رقم تليفون غير متصل بما يتيح القدرة لهذا الشخص لاستكمال هذه الخطوط غير المتصلة كما لو كانت خطوطه الخاصة، إنم الفوائد المترتبة على هذه التقنية تشمل تكلفة المكالمة التليفونية لتي تضاف إلى فاتورة التليفون غير المتصل، علاوة على منع حدود أو متابعة أو تقصي هذه المكالمة.

-2 تلاعب Pabx : وهو أسلوب تقني يمكن للشخص بموجبه أن يطلب رقم تليفون pabx (وهو صندوق تحويل معد يحتوي على عدد من خطوط التليفون المختلفة). ويتم من خلال توصيل مكالمتهم إلكترونيا لواحد من لخطوط في هذا الـ pabox ثم استعمال هذا الخط للأغراض الخاصة.

-3 الاتصال الخارجي بالكمبيوتر : وبموجب هذه الوسيلة يستطيع الشخص أن يتصل برقم تليفون معين يتيح لهم بدوره فرصة الوصول إلى نظام الكمبيوتر أو الوصول إلى مركز اتصالات يتيح لهم نفس المزايا الموضحة في الأسلوبين السابقين.

-4 Austpac : وهي شبكة اتصالات تشرف عليها هيئة المواصلات الرسمية التي تقدم وصلات معينة بين أنظمة الكمبيوتر، أن الفواتير الخاصة باستعمال هذا النظام تعتمد على استعمال شبكة التعرف على المستعملين Network User Identieication Cnut ويتكون هذا النظام عادة من سلسلة من 9 أرقام وهي شبيهة من حيث المبدأ برقم الـ PIN.

ويقصد بانتحال الهوية Iusurpation didentitie سرقة شخصية مستخدم آخر ويتطلب الوصل إلى الحاسب الآلي أو إلى الطرفيات معرفة دقيقة لمستعمل الجهاز.

وإن فحص الهوية يرتكز على مجموعة معلومات متوافقة يستخدمها المستعمل ككلمة السر[1] أو أي جملة خاصة بالمستعمل أو أي خاصية

-5 الغش في بطاقات الاعتماد : هذا الأسلوب التقني يتضمن اقتباس تفاصيل بطاقات الاعتماد الخاصة بأحد المشتركين الذي يقوم بدوره بطلب مكالمة تليفونية لصالح الطالب وقيد قيمة المكالمة على بطاقة الاعتماد.

-6 الاعتراض المادي : إن عملية الاعتراض المادي لخط تليفوني هي عملية بسيطة وتؤدي إلى نفس الفوائد مثل الاتصال بالنغمة.

-7 الوصلات غير القانونية : وهي عبارة عن تنشيط وتشغيل خدمة غير متصلة بدون علم شركة الاتصالات ثم استعمالها حسب رغبتك عن طريق تليفون عادي بدون أو تتلقي الفاتورة. وهذا النوع من الاعتراض يتميز بأنه دائم ومسمر.

-8 انظر :

Franklinclrk, investigating computer crime, Ed. CRC page 50.

(1) بعض كلمات السر يتم وضعها من خلال مدير النظام المعلوماتي والبعض الآخر يتم استخدامه من وحي المستخدمين أنفسهم. وبصرف النظر عن ذلك فإن كلمة السر يجب أن تكون مميزة لكل حساب ويجب تغيير وحذف الحسابات التي ليس لها كلمة سر وينصح بتجنب استعمال كلمات السر التي يسهل الوصول إليها مثل استعمال الأسماء الأولى والأخيرة وتاريخ الميلاد وأرقام الضمان الاجتماعي أو رقم رخصة القيادة فهذه الكلمات يمكن التنبؤ بها.

كما يعرف القراصنة كلما السر الأكثر شهرة والتي يميل الناس إلى اختيارها لذا يحظر استخدامها مثل كلمة سر passwred وكلمة ادخل Enter وافتح Open وكمبيوتر Computer ويحذر هذا الاستخدام كلمات السر المرتبطة بالهواية كما يحذر تجنب كلمات السر ذات المقطع الكبير أو تلك المتعلقة بمجموعة حروف أو أرقام.

فسيولوجية كالبصمة الرقمية أو ملامح للوجه أو هندسة الكف أو الصوت بالإضافة إلى أي شيء يمتلكه المستعمل كالبطاقة الممغنطة أو المفتاح المعدني.

فلو تمكن أي إنسان من الحصول على هذه المجموعة من المعلومات المتوافقة يصبح قادرا على انتحال شخصية المستعمل وهناك مثال لشاب ذكي أدعي أنه صحفي في إحدى المجلات واتصل بشركة اتصالات هاتفية مدعيا أنه بصدد نشر مقالة عن النظام المعلوماتي المستخدم في الشركة، فدعته الشركة لزيارة مقرها وقدم له موظفيها عرضا كاملا ومفصلا عن الأجهزة المعلوماتية وتطبيقاتها في الشركة وكانت النتيجة أنه سرق منهم معدات تزيد قيمتها على 10.000.000 دولار (مليون دولار) [1].

وفي حالة أخرى استطاع شخص أن يسرق بطاقات ائتمان ممغنطة لكل منها رقم سري يعرفه صاحبه حيث اتصل بأصحاب هذه البطاقات مدعيا أنه موظف بالمصرف وأخبرهم أنه قد نما إلى علمه أن بطاقاتهم قد سرقت وأنه بحاجة لمعرفة الرقم السري لحمايتهم وتزويدهم ببطاقات جديدة. وهكذا نجح المحتال في الحصول على الأرقام السرية لهذه البطاقات ثم استخدامها في سرقة مبالغ من المال من الموزعات الآلية للنقود[2] des distributeurs وفي حالة ثالثة أرسل فيها بعض الطلبة مذكرة لكل مستخدمي الطرفيات في جامعتهم ذكروا فيها أن أرقام الاتصال قد تغيرت ومنحوهم أرقاما جديدة تتصل مباشرة بأجهزة الكمبيوتر الخاص بهم والتي تمت برمجتها مسبقا بشكل مطابق لأجهزة الجامعة.

---

(1) انظر :

D. Parker, op. cit., p. 65.

راجع في ذلك :

E. Quarantiello (cybercrime) p. 94.

(2) المرجع والمكان السابقان.

وهكذا كان يستخدم المستعمل الرقم السري الخاص به بدون تردد حيث يسجله الطلبة ويعاودون مراسلتهم مرة ثانية طالبين منهم أن يعودوا لاستخدام رقم الاتصال القديم.

ولم تكن تلك سوي لعبة استخدام الطلبة من خلال كلمات السر most de pasdse .

ثالثا: السطو المسلح الإلكتروني

ترتب على ظهور تقنيات بث المعلومات على شبكة اتصالات بعدية telematique إلى نشوء مخاطر جديدة نتيجة للإمكانيات المستحدثة للدخول والاستفسار عن بعد من مراكز نظم المعلومات حيث تشكل عمليات بث المعلومات نقطة ضعف هامة في نظم المعلومات وذلك على النحو التالي:

1- التقاط المعلومات المتواجدة ما بين الحاسب الآلي والنهاية الطرفية :

يتيح هذا الالتقاط عن طريق توصيل خطوط تحويله un brnchement bretelles de derivaitions والتي ترسل إشارات إلكترونية "ذبذبات إلكترونية مكبرة" تمثل المعلومات المختلسة إلى النهاية الطرفية المتجسسة أو عن طريق مرسل صغير يسمح بنقل المعلومات من بعد.

وعلى النقيض عندما تسلك المعلومات الطريق الجوي "كما في حالة البث عن طريق القمر الصناعي" توضع هوائيات مطاردة بالقرب من الهوائيات الاحتياطية والتي تسمح بالتقاط الاشعاعات faisceux واحتجاز مضمونها.

2- التوصيل المباشر على خط تليفوني wiretape :

وقد سبق معرفة هذه التقنية في بعض المجالات وتباشر عن طريق وضع مركز تصنت unetable decoute يسهل تسجيل كل الاتصالات كما يمكن أن تؤدي هذه الوظيفة ميكروفونات صغيرة.

3- التقاط الاشعاعات الصادرة عن الجهاز المعلوماتي Electromagnetic pickup:

ويمكن عن طريق هذه التقنية إعادة تكوين خصائص المعلومات التي تتحرك وتنتقل من خلال نظام معلوماتي ويكفي لإتمام ذلك أن تسجل ثم تحل شفرة الاشعاعات الإلكترومغناطيسية المثبتة بواسطة أجهزة إلكترونية.

وفي الحقيقة تصدر بعض عناصر الأنظمة القوية وعلى وجه الخصوص الطابعات السريعة les imprimantesrapides أثناء تأدية وظيفتها إشعاعات الكترمغناطيسية، وقد ثبت أنه بإمكان شاحنة صغيرة مجهزة تجهيز خاص وقف بمحاذاة مبني مكتظ بالحاسبات الآلية، أن تلتقط وتسجل هذه الإشعاعات.

ويمكن عن طريق جهاز لفك الرموز أن يطلب من طابعة متصلة بنظيرتها الموجودة في المركز المستهدف النسخ الحرفي لنفس هذه المعلومات.

ويحضرنا في هذا الخصوص مثال شهير للسطو المسلح الإلكتروني وهو خاص باختلاس أموال عن طريق التقاط أمر بالتحويل مرسل من بنك إلى آخر وقد تمكن المختلس من تزييف الرسالة بالأمر بدفع نفس المبلغ لحساب فتح باسمه.

4- التدخل غير المشروع في نظام بواسطة طرفية phoneFreak :

يمكن عن طريق تقنية telematique التدخل في نظام معلوماتي من بعد ثم يصبح بعد ذلك نسخ أو تدمير بعض المعلومات شيئا سهلا ويكفي لبلوغ ذلك الحصول على حساب آلي ميكروي ومودم Modem ولتزود بكلمة السر أو مفتاح الشفرة المناسب[1].

(1) الدكتور محمد سامي الشوا، سابق الإشارة إليه، ص 68 وما بعدها.

رابعا: جرائم الحاسب من خلال التعدي على وظائفه

وتعدد أنماط هذه الجرائم على النحو التالي :

أ- تعديل المعطيات بدون إذن من صاحبه :

أصبح تعديل المعطيات le tripatouillage des donnees تقنية سهلة وآمنة ومألوفة من تقنيات الإجرام المعلوماتى وهي تتمثل في تعديل المعطيات قبل أو أثناء إدخالها في نظم المعلومات أو في لحظة إخراجها من النظام المعلوماتي.

ويمكن إجراء هذه التعديلات بواسطة أي شخص والذي ساهم أو له حق الولوج في عمليات نشاء وتشفير وتسجيل ونقل والتحقق من نقل البيانات المخصصة للإدخال في نظم المعلومات وهناك العديد من الأمثلة التي تنطوي على تزوير أو اختلاس الوثائق واستبدال الشرائط المغنطة[1] أو البطاقات المثقوبة أو أفعال تحطيم إدخال البيانات أو إحداث ثقوب إضافية في البطاقات المثقوبة أو على العكس سد هذه الثقوب وأخيرا أفعال التحييد أو إلغاء المراقبات اليدوية[2].

وأجريت في انجلترا ما بين عامي 1983 و 1986 دراسات مسحية قام بها Wong تتعلق بحالات الاحتيال في نظم المعلومات حيث تبين من خلالها أن 63% من الحالات محل الدراسة قد ارتكبت عن طريق التلاعب في

---

(1) الشريط الممغنط : وهو شريط مغناطيسي يحوي المعلومات الخاصة بحامل البطاقة بعد تشفيرها بصورة إلكترونية ويمكن قراءة هذه البيانات باستعمال النهاية الطرفية الإلكترونية الموجودة بمقار البنوك ومنافذ البيع.

Document that is being prepared with a view to submission to the Europen Union in Brussels.

(2) انظر في ذلك :

D. parker Op. Cit. p. 77

البيانات المدخلة أو في الوثائق الأصلية التي تستمد منها البيانات، وأن أبرز أشكال هذا التلاعب تم عن طريق تحويل المدفوعات من حساب إلى حساب آخر أو بوقف سداد المستحقات أو باصطناع موردين أو عملاء وهميين لهم مستحقات واجبة السداد أو بوضع أسماء زائفة لبعض الموظفين يستحقون أجورا ومرتبات[1].

ومن تحليل إجراء معهد ستانفورد الدولي للأبحاث (SRI) بالولايات المتحدة شمل مائة حالة من حالات إساءة استخدام الحاسبات، تبين أن 37.6% منها قد ارتكب بإحداث تغيير مباشر direct modification في البيانات المدخلة بينما وقع 9.5% منها فقط نتيجة تعديل وتلاعب في البرامج المستخدمة[2].

ومن الحالات الواقعية لجرائم الحاسب الآلي والتي ارتكبت باستخدام هذا الأسلوب ما يأتي :

قامت إحدى موظفات أحد فروع بنك ادخار بجنوب ألمانيا بتحويل مبلغ 1.3 مليون مارك ألماني عام 1983 إلى حساب صديقها من خلال إدخال بيانات غير صحيحة إلى حاسوب البنك عبر النهاية الطرفية الموجود بمكتبها.

(1) وهكذا استطاع أحد المسئولين عن نظم المعلومات بإحدى الشركات الفرنسية اختلاس أكثر من مليون فرنك فرنسي عن طريق إعادة ملفات الموظفين السابقين والذين لهم حقوق مالية وقامت بتحويلها إلى حسابه وحسابات أخرى تم افتتاحها خصيصا لهذا الهدف وبعد ارتكاب الجريمة قام المجرم بمحو آثار كل فعل عن الغش المعلوماتي :
راجع في ذلك : Expertises no. 66 oct. 1984 مشار إليه في : د. محمد سامي الشوا، سابق الإشارة غليه، ص 73.

(2) راجع في ذلك الدكتور هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، طبعة 1994، ص 59.

وقد اكتشفت أنظمة الأمن والرقابة المتطورة التي يستخدمها البنك عدم صحة هذا التحويل في ظهر ذات اليوم لكن الإرسال الفوري المباشر (online) للتحويل والسرعة الفائقة في إجراء العمليات المالية عن طريق الأجهزة الإلكترونية الحديثة، أتاح لصديقها بعد بضعة دقائق من قيامها بالتحويل، صرف ثلاث شيكات من فرع آخر للبنك بمبلغ 1.28 مليون مارك[1].

قام موظف يعمل في مجال معالجة البيانات (قسم الحاسوب) في أحد البنوك السويسرية الكبري، بالتلاعب في المعاملات المالية الخارجية للمصرف، والاستيلاء مع بعض شركائه على مبالغ طائلة، وكان يمنع، بحكم عمله كمشغل ومراجع بيانات، وصول بعض أوامر تحويل النقود إلى قسم الترميز ebcidubg deoartlebt ليقوم هو بعملية إدخالها إلى الحاسب غير أنه بدلا من إدخال القيمة الفعلية لكل أمر تحويل كان يدخل هذه القيمة مضروبة في ألف، وقد تمكن بهذه الطريقة من الاستيلاء على (700.000) فرنك سويسري من أموال البنك[2].

وهناك حالة ثالثة لموظفة تدعي سارة تعمل في إحدى الشركات وهي مسؤولة عن عملية المراجعة pointage حيث يتمثل هذا العمل في ملئ استمارات كل موظف تثبت فيه عدد ساعات عمله القانونية والإضافية وأسمه ورقمه كما أنها تصحح استمارات الأسبوع السابق وتتأكد من صحة البيانات وتنقل عن طريق آلة التثقيب من الاستمارة إلى البطاقة المثقوبة ثم يقوم بعد ذلك الموظفين بجمع هذه البطاقات المثقوبة حيث يتم حصرها وجمع عدد الساعات بواسطة آلة حاسبة.

---

(1) انظر د. هشام رستم، سابق الإشارة إليه ص 60.

(2) المرجع والمكان السابقان.

ويتم تثقيب عدد من البطاقات ويثبت مجموع الساعات على كل بطاقة ثم تنقل البطاقات بعد ذلك إلى مركز الحاسب الآلي لمعالجتها حيث يقوم هذا الأخير بتنفيذ برنامج الساعات الإضافية والأجور في نهاية كل أسبوع وتطبع الشيكات في الأسبوع التالي.

وكانت سارة شغوفة لمعرفة أسلوب عمل كل جهاز وليس عملها فقط كما كانت رأسها مليئة بالأفكار الجريئة وعينها تراقب العملية اليدوية فأيقنت أن كل المراجعات وتصحيح المعطيات تقوم على أساس واحد هو اسم الموظف كما لاحظت أن أرقام الهوية المدونة على الاستمارة لا تستخدم أبدا.

وبدأت سارة القيام بأولي محاولاتها الفردية فوضعت اسم موظف ورقم موظف آخر على استمارة وانتظرت لتعرف النتيجة حيث تلقت تقرير مطبوع على الكمبيوتر يخبرها بوجود حالة شاذة فقد ذكر الكمبيوتر أن الموظف الذي سجلت رقمه عمل 80 ساعة قانونية أي ضعف الحد الأقصى لساعات العمل وعلى ما يبدو فقد كشف نظام الكمبيوتر الخطأ على أساس أن أحد لا يستطيع أن يعمل أكثر من 40 ساعة ثم تساءلت سارة عما قد يحدث لو استخدمت أسماء الموظفين الذين عادة ما يعملون عدة ساعات إضافية وسجلت مع أسماءهم أرقامها هي، ثم سجلت عدة ساعات إضافية على استمارات إضافية حيث توقعت أن يسجل لها الكمبيوتر هذه الساعات الإضافية طالما أن رقمها هو المدون على الاستمارة. وبدأت التنفيذ واحدة وعدد من الساعات وانتظرت الأسبوع الآلي حيث موعد صرف الشيكات. وفي يوم الجمعة فتحت مظروف مرتبها ووجدت أجر الساعات الإضافية التي لم تعملها مضافا إلى مرتبها. ولم تحاول سارة أن تبلغ الإدارة عن هذا الخطأ وانتهزت فرصة المال السهل واستطاعت أن تحصل على عدة آلاف من الدولارات كل عام وأثناء قيام أحد مفتشي الإدارة بتصفح استمارات الدخل السنوي للموظفين تعجب من ارتفاع راتب سارة بهذا الشكل الملحوظ، فبدأ فضوله يدفعه بطرح العديد من الأسئلة وإلى مراقبة السجلات وتأكد من عملية

التحايل ثم اعترفت سارة بهدوء أمام المفتش بهذا العمل غير المشروع حيث ذكرت في البداية أنها كانت سعيدة للمخاطرة لكن الموضوع تحول بعد ذلك إلى روتين ثم على قلق في الشهور الأخيرة.

وأعادت سارة للإدارة المبالغ التي حصلت عليها في السنة الأخيرة وبدأ عليها الندم وهي تصف عملية التحايل بالتفصيل.

وشعر المفتش الإداري بخيبة الأمل وهو يستمع إلى مدي بساطة أسلوب سارة وبدأ يفكر في ضرورة إصلاح الخطأ وتعديل البرامج تعديلا جوهريا ولكن وجد أن ذلك يحتاج إلى مبالغ باهظة وفي النهاية اضطر لتأجيل عملية الإصلاح بأكملها والغريب أن سارة حصلت على ترقية ومرتب أعلى بعد أن وعدت بعدم كشف الأسلوب الذي اتبعته في السرقة[1].

ب - تقنية Superzapping :

يطلق مصطلح Superzapping على تقنية الاستخدام بأسلوب غير شرعي للبرامج الخدمية التي تؤثر على المعطيات المحفوظة في جهاز الكمبيوتر أو في ذاكرته وهذا التأثير قد يكون بالتعديل أو الإلغاء أو النسخ أو الإدخال أو الاستعمال أو المنع.

ومصطلح Superzapping مشتق اسمه من Superzap وهو البرنامج الخدمي الذي يستخدم في العديد من مراكز نظم المعلومات كأداة نظام. وأي مركز نظم معلومات يسر وفقا لخطة عمل ناجحة وفعالة لابد له من برنامج يلجأ إليه عند الحاجة بغرض التعديل أو الكشف عن أي غموض في جهاز الكمبيوتر.

---

(1) راجع في ذلك :

D. Parker op. cit. p. 81

وأحيانا تتوقف أجهزة الكمبيوتر أو لا تعمل بالكفاءة المرجوة ويصبح إصلاحها أو إعادة تشغيلها غير مفيدة وأحيانا أخرى يحتاج الكمبيوتر لعملية تعديل لا تسمح بها أساليب الولوج المألوفة. وفي مثل هذه الحالات فإن برامج الولوج الإجمالية تكون ضرورية، حيث يمكن تشبيهها في مثل هذه الأحوال بمفتاح يستخدم في حالات فقد كل المفاتيح الأخرى.

وهذه النوعية من البرامج الخدمية لها القدرة على فعل كل شيء وهي في نفس الوقت أدوات خطيرة إذا وصلت إلى أيدي أشخاص غير شرفاء لهذا يجب الحفاظ عليها بعناية ويجب أن توضع بمنأى عن المستخدمين غير الشرعيين. لكننا أحيانا نجدها في مكتبات البرامج، لذا فإن أي شخص سواء كان مبرمجا أو مشرفا فنيا والذي يعرف استخدامها ومكانها فإنه يمكنه الحصول عليها. وهناك مثال على سرعة هذا البرنامج تسبب في خسارة مقدارها 128.000 دولار من أحد البنوك التي تقع في ولاية نيوجرسي حيث كان رئيس قسم الاستثمار لهذا البنك يستخدم برنامجا من نوع Superzap لإجراء بعض التعديلات في الحسابات الراكدة le solde des comptes وتصحيح الأخطاء وفقا للتوجيهات الممنوحة له من الإدارة حيث لاحظ أن التصحيح لا يتم على أحسن وجه.

وفي أثناء محاولاته أيقن أنه من السهل إجراء التعديلات دون التعرض لأية رقابة ودون ترك أي دليل على قوائم المعطيات فبدأ يحول مبالغ إلى حسابات ثلاثة من أصدقائه وهو واثق أن الوسائل التكنولوجية ستعجز عن اكتشاف الاحتيال[1].

(1) راجع :

D. Parker, op. cit., p. 85.

ج- تقنية الاسترجاع **Recuperation** :

وهي عبارة عن تقنية يستخدمها شخص من أجل الحصول على معلومات موجودة في نظام معلوماتي أو قريبة من نظام معلوماتي بعد تنفيذ عمل ما.

ويمكن أن يتمثل الاسترجاع البسيط والمادي في التفتيش في سلات المهملات لأجل الحصول على نسخ من القوائم الملقاة فيها أو العثور على ورقة كربون المستخدم في نسخ تلك القوائم وتستلزم الأساليب الأكثر تقنية وخداعا للاسترجاع ضرورة البحث في المعطيات الموجودة داخل الحاسب الآلي بعد تنفيذ عمل ما، وعلى سبيل المثال لا يمكن لنظام التشغيل un systeme d'exploitation أن يمحو مناطق الذاكرة المغلقةles zones de memoiretampn والمستخدمة بواسطة الذاكرة المؤقتة لمعطيات الإدخال أو الخروج.

وهناك بعض أنظمة التشغيل التي لا تمحو مضمون ذاكرة الاسطوانة أو الشريط الممغنط والسبب في ذلك أن هذا العمل يستغرق وقتا كبيرا. لذا فإن المعطيات الجديدة يتم كتابتها فوق المعطيات القديمة. ومن ثم يمكن بسهولة قراءة هذه المعطيات القديمة قبل أن يحل محلها المعطيات الجديدة. فإذا ما تم حفظ الذاكرة واستخدمت في عمل سابق ثم أسند إليها عمل جديد، فإن هذا الأخير يمكن من خلاله الولوج إلى نفس الذاكرة ولا يكتب إلا القليل من المعطيات لموجودة بهذه الذاكرة ولكن يمكن بعد ذلك أن يعيد قراءة كل محتوي الذاكرة المستولي عليها أو استعادتها، وكذلك البيانات المختزنة بواسطة العمل السابق.

وكان عدد من شركات البترول - كعملاء يتبع إدارة المشاركة بالوقت، ولاحظ المسئول عن قسم تشغيل الحاسب الآلي أنه في كل مرة يستخدم فيها أحد العملاء الخدمات المعلوماتية، فعليه أن يستخدم شريط جديد للعمل، وهذا

يؤدي إلى أن القائم على نظام التشغيل يقرأ المعطيات الموجودة على الشريط قبل أن تكتب عليها أي شيء ولما تكرر هذا الأمر أثار دهشته رفع الأمر إلى إدارته وبعد تحرياته البسيطة تبين أن العميل كان يقوم بالتجسس الصناعي ويحصل على البيانات من الذاكرة الخاصة لمختلف شركات البترول، وهي بيانات مسجلة على شرائط ثم يقوم ببيع هذه المعطيات الثمينة لشركات بترولية منافسة[1].

د- تقنية Chausse – trapes, techniques du cheval de troie et de salami

1- chausse – trapes :

يقوم المبرمجون في مجال البرامج التطبيقية programmes d'application والتي تقوم بمعالجة البيانات الخاصة بالإدارة وأنظمة التشغيل والتي تنحصر مهمته في ضمان تشغيل أنظمة المعلومات بإدخال برامج اختبار وإضافة تعليمات تكميلية وأساليب للحصول على نتائج وسيطة ويمكن تشبيه هذه المساعدات بالسقالات المستخدمة في بناء المساكن. ومن بين أهداف نظام التشغيل مراقبة الولوج إلى النظام المعلوماتي من جهة، ومن جهة أخرى ضمان التحكم في استخدامه على نحو دقيق. وعلاوة على ذلك فهو لا يسمح لا بالتعديل ولا بإدخال تعليمات إلا باستثناء الحصول على تصريح لازم لمباشرة ذلك.

والذي يجب أن يكون على قدر من الدقة ويطبق حرفيا، ومن ثم فإن مبرمجي النظام يدخلون أحيانا أساليب منطقية ومؤقتة كي تسمح لهم بتخطي هذه القيود أثناء مراحل الاختبار وتزايد البرامج أو في مرحلة تأتي بعد ذلك عند صيانة النظام أو تعديله.

(1) Parker, op. cit. p. 86.

ويتغاضي المبرمجين أحيانا عن أخطاء موجودة في برامجهم وهذه لا يتم اكتشافها إلا في مرحلة الاختبار وتصبح بعد ذلك مهملة وعندئذ يضعون مختصرات والتي تخترق أساليب تصحيح البرامج وشروط استخدام النظام. وعلى سبيل المثال حينما يقوم برنامج يدعي "X" بالاتصال ببرنامج يدعي "Y" فإن المعطيات اللازمة لبرنامج "Y" فقط هي التي يجب أن تكون على قدر كبير من سهولة الوصول إليها.

وقد تكون الجهود الخاصة بالبرمجة اللازمة لجمع كل البيانات على قدر من الصعوبة في حين أن هناك تقنية على قدر كبير من البساطة ولكنها تبرهن على الإهمال وتتمثل في جعل المعلومات سهلة الوصول إلى البرنامج "Y" حيث يرشده إلى الأماكن الخاصة بالمعطيات والتي تسمح للبرنامج "Y" بالولوج إلى منطقة معطيات قريبة جدا وأكثر من اللازم، وهذا ينطوي على مخالفة مبدأ الامتياز الأقل moindre privilege.

والذي يقلل من معدل أمان النظام، وتبقي البرامج متزامنة في الذاكرة ويجب أن تصمم على نحو بحيث يحذر إحداها الأخرى كما لو كانت داخل بيئة عدوانية. والخسائر التي يمكن أن يسببها أي برنامج دخيل يجب أن تكون على نحو ضئيل.

ويمكن أيضا لمصممي البرامج الضخمة التدخل عن طريق السهو ومواطن الضعف وبسبب أوجه القصور على مستوي البرنامج أيضا.

وعلى سبيل المثال فمن المألوف بصفة دورية عمل نسخ احتياطية تكميلية لمحتويات وحدة الذاكرة الأولية doit etre maintenuou vameliore وذلك أثناء تنفيذ الأعمال الممتدة للإنتاج وتخزن هذه النسخة على وحدة ذاكرة ثانوية (وهي عبارة عن شريط ممغنط أو إسطوانة) وذلك من السماح بإعادة تكوين البطاقات وإعادة التشغيل في حالة حدوث أي عطل طارئ، وذلك بهدف تجنب إعادة تنفيذ هذا العمل كله. وفي الأنظمة ذات

التصميم المتواضع، فإن العلامات يتم نسخها أيضا. ثم إعادة تكوينها فيما بعد استنادا إلى النسخة الاحتياطية في حالة حدوث عطل ويمكن أثناء هذه الفترة إعادة تكوين النسخة الاحتياطية بتعديل البيانات الخاصة بمفتاح الشفرة.

وهكذا، يمكن لبرامج النسخة الاحتياطية أن تكون لها القدرة على الولوج في مناطق أكثر اتساعا للبيانات. ويمكن أيضا إحداث أفعال تعدي في الدوائر الإلكترونية وعلى سبيل المثال يمكن لتلك الدوائر أن تنفذ مجموعات متوافقة للتشغيل ولكنها غير متوقعة مما يعرض النظام للخطر.

ويكتشف المبرمجون المهرة - عند استخدام وصيانة البرامج والدوائر - بعض الفخاخ سواء لأجل تحقيق غايات مفيدة أو لتنفيذ أعمال غير مشروعة[1].

وهناك أمثلة متعددة لاستخدام هذه التقنية ومنها ما يأتي :

الحالة الأولى : اكتشف أحد مبرمجي النظم فخا داخل مصنف Fortran حيث يسمح الفخ للمبرمج الذي يستخدم لغة Fortran في الكتابة بتحويل التحكم في برنامجه إلى ذاكرة تستخدم للبيانات على النحو الذي أدي إلى تنفيذ الكمبيوتر لتعليمات تتكون من بيانات يطلبها المبرمج. فأصبح بمقدور هذا الأخير أن يصدر تعليمات سرية تنفذ بشفرة الآلة عن طريق إدخال معطيات محددة كلما استخدم برنامج Fortran. وسبق أن تم ذلك في إحدى الشركات التجارية للمشاركة بالوقت، حيث استطاع مبرمج نظم بالتواطؤ مع موظف بتلك الشركة أن يستخدم الحاسب الآلي لعدد كبير من الساعات مجانا وبالأسلوب السابق ذكره تمكن من الحصول على معطيات وبرامج تعمل بنظام المشاركة بالوقت.

---

(1) انظر في ذلك :

D. Parker, op. cit. p. 93

الحالة الثانية : ومن خلالها اكتشف بعض مهندسي السيارات وجود فخ في برامج إحدى الشركات التي تعمل بنظام المشاركة بالوقت في ولاية فلوريدا مما سمح لهم بالحصول على كلمة السر المميزة وأصبح في مقدورهم الحصول على نسخ من البرامج التجارية السرية وشرعوا في استخدامها مجانا[1].

2- Cheval De Troie (حصان طروادة):

إن هذا المصطلح الأسطوري يضفي طابع كلاسيكي على هذه الوسيلة الإجرامية والذي لم يتم اكتشاف سوي حالات قليلة من هذا النوع من الجرائم، ولكن يكثر الحديث عن هذه التقنية نظرا لنجاحها في غالبية الأحوال، وأن هناك عدد ضئيل من الذين يملكون المهارة والمعرفة لممارسة هذه التقنية أو لوجود تقنيات إجرامية أسهل وأقل حرفية مثل تقنية إتلاف المعطيات.

وبرنامج حصان طروادة يتمثل في إدخال أوامر وعلى نحو غير مشروع إلى الحاسب الآلي بهدف تحقيق أغراض إجرامية[2].

كيفية مباشرة تقنية حصان طروادة :

يمكن عمل برامج لاستخدام تقنية حصان طروادة[3]، وذلك عن طريق

---

(1) انظر في ذلك :

D. Parker, op. cit., p. 94

(2) بدأ هذا البرنامج في الظهور حسبما يقرر البعض في الولايات المتحدة الأمريكية في أواخر السبعينات نتيجة لانتشار استخدام اللوحات الإلكترونية للبيانات والتي تتيح بدورها إما تخفيف أو زيادة تحميل البرامج. راجع في ذلك : د. هشام رستم، سابق الإشارة إليه ص 71 وما بعدها.

(3) برامج حصان طروادة : وهي تلك البرامج التي تبدو وكأنها قطع جذابة مضافة إلى البرامج، إلا أنها تملك القدرة على الإضرار بالبيانات وعلى عكس الفيروسات فهي لا تقوم بنسخ نفسها آليا.

إدخال تعليمات في أحد البرامج أثناء تكوينه أو بإدخال تعليمات في وقت لاحق في لغة المصدر language source أو في إدخال تعليمات في لغة الآلة (ولكن هذا يستلزم مجهود ضخم وذلك في المرحلة التي يتم فيها التنفيذ بواسطة الحاسب الآلي).

وعادة ما تحفظ ترجمة لغة المصدر على شريط أو اسطوانة ممغنطة في مكتبة المصدر ويتعين استخدام الشريط أو الاسطوانة وكذا برنامج تحديث لإجراء التعديلات والدخول ومن ثم يمكن الحصول على شريط جديد أو اسطوانة جديدة وإعادة الأصل المستخدم إلى المكتبة ونسخة حصان طروادة لا تستخدم إلا عندما يكون البرنامج قد انتحل لغة الآلة. وهكذا يحل محل نسخة الإنتاج المستخدمة حتى ذلك الحين.

ولتحويل البرنامج - المكتوب بلغة الآلة والمستخدم في الإنتاج - إلى حصان طروادة فيجب أن يحل البرنامج في المكتبة محل برامج الإنتاج والتي عادة ما تحفظ على أشرطة أو اسطوانات والتي بدءا منها يتم مباشرة تحميل البرامج في الذاكرة، وهناك حل آخر يتمثل في إدخال تعليمات سرية وعلى نحو تعد جزءا من تعديل أو من بطاقات تحديث تحفظ عادة على بطاقات مثقوبة أو أشرطة وهكذا تدخل إلى الحاسب الآلي في كل مرة يستخدم فيها البرنامج.

إخفاء حصان طروادة :

يمكن كشف التعديل الدائم أو شبه الدائم للبرنامج إذا ما تم فحص البرنامج يدويا أو إذا استخدم الحاسب الآلي لعمل مقارنة آلية مع النسخة الأصلية.

=

راجع في ذلك :

Dr : Linda Volonino Cyber Tevrorism op. cit.

ولآجل تجنب هذا الكشف فهناك تقنية على قدر كبير من الصعوبة وتتمثل في إدخال تعليمات سرية وربما أدمجت في برنامج آخر والذي دائما ما يستخدم أثناء عمل برنامج الإنتاج في الذاكرة.

ويمكن أن يكون المحتوى في حالة حصان طروادة هذا عبارة عن برنامج نفعي programme utilitaire للاختيار أو للطبع أو برنامج يستخدم في ترجمة برنامج لغة المصدر إلى لغة الآلة وعندما يتم تنفيذ المحتوي فإن تعليمات حصان طروادة تجري تعديلا أو إدخالا مؤقتا لتعليمات عديدة في برنامج الإنتاج وذلك قبل تنفيذ الجزء المعدل وإلغاء هذا الجزء بعد ذلك عقب تنفيذه[1].

وعادة ما توجد برامج حصان طروادة في برامج الأعمال كبرامج معالجة النصوص وبرامج إدارة قواعد البيانات وغالبا ما تكون مختفية في منتصف البرامج أو في مكان غير مستعمل منه. والبرنامج الذي يتضمنها قد يعمل بطريقة صحيحة لعدة شهور قبل أن تظهر الأوامر الغير متوقعة وقد تظهر هذه الأوامر وتنفذ مباشرة عند تشغيله.

(1) ومن قبيل ذلك أن يدس تعليمات في الخفاء في البرامج المستخدمة لإصدار شيكات لمستحقيها بصفة دورية (كأرباب المعاشات مثلا) وإرسالها إليهم عن طريق البريد وتكون مهمتها تحريف الإخطار الذي يجري إدخاله إلى الحاسب بوفاة مستحق الشيك والذي يترتب عليه وقف إصدار شيكات باسمه في المستقبل لتجعله إخطارا من مستحق الشيك بتغيير عنوانه مؤقتا لمدة ثلاثة شهور متتالية وهكذا يصدر الحاسب خلال هذه الشهور شيكات باسمه ترسل إلى العنوان المؤقت الذي يكون معد هذه التعليمات قد حدده ورتب أمر قيامه باستلامه والاستيلاء على قيمته.

وبعد انقضاء الشهور الثلاثة تعيد التعليمات المخبأة في البرنامج البيانات التي جري تحريفها إلى أصلها لتكون إخطارا بوفاة مستحق الشيك وهو ما يجعل اكتشاف أمر هذا التلاعب بالغ الصعوبة.

راجع في ذلك : د. هشام رستم، سابق الإشارة إليه، ص 72-73.

وسمي هذا البرنامج بحصان طروادة للدلالة على خطورته وآثاره المدمرة وقدرته على الخداع[1] والمفاجأة والتضليل مثلما كان حصان طروادة الخشبي الكبير الذي ضم بداخلة مجموعة من الجنود قد أحكم خداع جيش طروادة وهي تدافع عن أرضها حيال غزو أسبرتا لها وفقا لما جاء بقصص الحب التي رواها الشاعر الأغريقي القديم هرميروس في ملحمتي الإلياذة والأوديسة[2].

أمثلة واقعية لتقنية حصان طروادة :

المثال الأول :

هناك رجل يدعي John Mccloud يبلغ من العمر 30 عاما وكان يعاني العديد م المشاكل، حيث فقد أولا عشيقته ثم فقد بعد ذلك مهنته وتراكمت عليه الديون بسبب إدمان القمار وباءت عدة محاولات للاستثمار من جانبه بالفشل وكان أمله كبير في سداد تلك الديون. وكان Mccloud يعمل كمهندس استشاري ومبرمج في شركة أموال مالية في إحدى مدن الجنوب الأمريكي حيث عرف الناس الممارسات الغير راعية في قطاع الأعمال وقد دفعت هذه العوامل جميعها cloud إلى ارتكاب جريمة معلوماتية لم يستطع تفاديها، حيث كانت الشركة تبيع الأوراق المالية (نوع من الشيكات مقبولة الدفع بواسطة مندوبين يغطون عدد كبير من المدن) وعندما يشتري العميل تلك الأوراق المالية تسجل القيمة المطبوعة عليها وسعرها في حسابات الشركة المدينة ثم يسدد بها العميل ديونه لشخص آخر ويقوم هذا الأخير بإرساله إذن الصرف للشركة ويتسلم القيمة المدونة عليه. وتستعين الشركة بمحاسب مسئول عن تلك الأوراق المباعة والمشتراة.

---

(1) راجع في ذلك : د. هدي حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، 1992، ص 102-103

(2) راجع في ذلك : د. هشام رستم، سابق الإشارة إليه ص 73-74.

ثم قرر Jimmy Saturn مدير الشركة أن يتخلي عن المحاسب وأن يقتني نظام معلوماتي Datapoint 5500 في أغسطس 1980 حيث أبرم Jimmy عقدا من أجل تطوير البرنامج مع إحدى الشركات المتخصصة في نظم المعلومات وهنا ظهر Cloud على المسرح، حيث قام ببرمجة نظام التطبيقات لجميع الأوراق المالية في نظام Datapoint 5500 ولكن الشركة استغنت عنه بمجرد الانتهاء من هذا العمل، ثم استعان به Jimmy مرة أخري من أجل تصليح بعض الأخطاء الموجودة في البرنامج وفي هذه اللحظة تفاقمت مشاكل Cloud وعلى وجه الخصوص متاعبه المالية مما جعله يفكر في ارتكاب أفعال الاحتيال. وتنفيذا لفكرته أدخل Cloud في البرنامج ستة تعليمات خفية بلغة bacic تتيح له تغذية الحاسب ببيانات عن تعاملات وهمية للشركة لكي تعالج وتخزن تحت رمز "E" لأحد ملفات البرنامج وبحيث لا تظهر البيانات المدخلة والمعالجة تحت هذا الرمز في مستخرجات الحاسب.

ومع أن مدير الشركة كان باستطاعته قراءة هذه التعليمات المضافة وإدراك دلالتها إلا أنه لم يفعل لفرط ثقته في Cloud، خاصة وأن الأخير كان قد أخطره أنه قد أدخل الرمز "E" في البرنامج ليدرج تحت بيانات وهمية - تمحي فيما بعد - بغرض تجربة البرنامج والتأكد من دقة أدائه لمهامه، وهوة إجراء يجري في العادة إتباعه لاختبار مدي صحة عمل البرامج.

وارتكز خطة Cloud في اختلاس أموال الشركة على سرقة بطاقات الأمر بدفع النقود وإدخال بيانات إلى الحاسب تحت الرمز "E" ثم تعبئتها ببياناته الشخصية والتوجه إلى البنك بعد ذلك لتحصيلها، وبهذه الطريقة كانت البيانات الخاصة بهذه البطاقات تدرج فحسب، داخل نظام معلومات الحاسب دون أن يكون لها أي أساس فعلي، ودون أن تظهر في المستخرجات

المطبوعة للحاسب، ورغم أن هذه البطاقات كانت تحمل أرقاما متسلسلة، إلا أن سرقتها لم تكن تثير انتباه المراجعين بالشركة لشيوع اعتقاد بينهم بإمكانية فقدها أثناء عملية الانتقال إلى النظام المحاسبي الجديد أو أثناء عمليات تداولها بالبريد.

وتجنبا لظهور عجز في ميزانية الشركة نتيجة الاستيلاء على أموالها، عمد Cloud إلى تغطية هذا العجز كلما توافر لديه مال، حيث كان يسدد باسم وهمي مالا للشركة يدخله في نظام حاسبها تحت الرمز "E" بيد أنه لم يتمكن في إحدى المرات من تغطية عجز ظهر بحسابات الشركة فاق مجموعه 100.000 دولار. مما دعا مدير الشركة إلى تكليف المختصة بمراجعة الحسابات بفحص الأمر لاكتشاف مصدر الخطأ المسبب للعجز وتصحيح الحسابات غير أن الأخيرة تقاعست عن القيام بذلك لمدة ثلاثة شهور، ثم قامت تحت إلحاح مدير الشركة بتحديد يوم معين (7 مايو 1981) لبدء عمليات الفحص والمراجعة.

ولأن عمليات الفحص والمراجعة كان يمكن أن تسفر عن كشف تلاعبه فقط اضطر Cloud إلى اللجوء إلى الوسائل التقليدية لإخفاء معالم جريمته حيث اقتحم ليلا في اليوم الساق على موعد إجراء الفحص والمراجعة مقر الشركة وقام بسرقة بعض الوثائق المثبتة لإدانته وكان منطقيا أن يركز البوليس في تحقيقاته، بعد إخطاره بالاقتحام والسرقة صباحا،على طبيعة المسروقات وأهميتها والدافع وراء سرقتها وهو ما قاده إلى الاشتباه في Cloud الذي استشعر صعوبة موقفه فبادر إلى الاعتراف بجريمته عند مواجهته[1].

(1) انظر في ذلك : D. Parker سابق الإشارة إليه، ص 100 – 101 .

المثال الثاني :

لم تعرف سوي حالة واحدة لإدخال تقنية حصان طروادة إلى الدوائر الإلكترونية وأول حالة تم التبليغ عنها كان في نوفمبر 1981 حيث تم القبض على رجلين في وسط السويد يبيعان الزهور في محل صغير ولم يكن هذا العمل سوي ستار لبيع دوائر مطبوعة بديلة بالدوائر المستخدمة في الآلات التي تقبل النقود الورقية لشراء الوقود.

وأمكن عن طريق تلك الدوائر المطبوعة المقلدة الحصول على الوقود مجانا وانتشرت هذه الحيلة في السويد كلها مما تسبب في إلحاق خسائر جسيمة في محطات الوقود[1].

هـ- تقنية SaLAMI :

وهي إحدى أنماط الجرائم الآلية التي تنطوي على سرقة مبلغ بسيط من المال يتم تحصيله من مصادر متعددة (وهي على منوال أخذ شرائح صغيرة بدون انقاص الجزء الأكبر بشكل واضح وعلى سبيل المثال ففي أحد البنوك حيث يسمح نظام المحاسبة بالإطلاع والتحقق من الحسابات أمكن تغييره (باستخدام أسلوب حصان طروادة لاستقطاع بضعة سنتيمات من عدة حسابت وتحويل هذه المبالغ إلى حساب معين حيث يمكن السحب منه وعلى نحو مشروع. وهكذا لا يوجد اختراق على مستوي أساليب المراقبة لأن النقود لم تسحب على نحو غير مشروع من النظام المحاسبي.

وعلى النقيض فإن جزءا صغيرا من المال أعيد توزيعه مرة أخري بدون قيد أو شرط ويرتكز نجاح فعل الغش على حقيقة مؤداها أن كل عميل يتحقق من حسابه المفقود إذا كانت النتائج جسيمة أما إذا كانت خسارته ضئيلة فلا يهتم بها.

---

(1) D. Parker ، سابق الإشارة إليه ص 101.

وقد أطلق على هذه التقنية مصطلح Perruque بسبب استقطاع سنتيم بسنتيم، على نمط الحلاق الذي ينجز عمله شعرة بشعرة، وتطبق أحيانا في البنوك والتي تمنح فوائد للحسابات الجارية[1].

ولا تستخدم تقنية SALAMI في قطاعات الأعمال الصغيرة لتي لا يوجد بها عدد كاف من الحسابات. بل إن مجالها المفضل هو القطاعات المصرفية التي تعتمد أعمالها على النظم المعلوماتية، حيث يمكن إدخال تغييرات في البرامج المستخدمة لاقتطاع مبالغ زهيدة القيمة من عدة مئات من الحسابات وتحويل هذه المبالغ إلى حساب خاص للمحتال حيث يقوم بالسحب منه وفقا للطرق والإجراءات المعتادة[2].

وقد يصل الأمر أحيانا بالمبرمجين من ذوي الميول الإجرامية إلى زرع برنامج رعي غير مسموح به في البرنامج الأصلي، ومعروف لهم فقط ويسمح لهم بالولوج غير المشروع في موردات (وهي عبارة عن العناصر الضرورية اللازمة لتشغيل نظم المعلومات) الحاسب الآلي.

ويمكن وضع هذا البرنامج الصغير السري وبمهارة بين آلاف التعليمات التي تكون برنامجا معلوماتيا.

ومن أمثلة استخدام تقنية Salami ما يأتي :

قام مبرمج يعمل بأحد البنوك بتعديل برنامج إدارة الحسابات الخاصة بالبنك وبحيث يضيف عشرة سنت لمصاريف إدارة الحسابات الداخلية على

---

(1) انظر في ذلك :

B Lussato, le defi informatique ed Fatyard.

(2) راجع في ذلك :

D. Parker, op. cit., p. 103.

د. جميل عبد الباقي الصغير – القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناتجة عن استخدام الحاسب الآلي، الطبعة الأولي، 1992، دار النهضة العربية، ص 47.

كل عشرة دولارات ودولار واحد على الحسابات التي تتجاوز عشرة دولارات. وتم تسجيل المصاريف الزائدة في حساب خاص فتحه باسم مستعار Zzwicke.

وهكذا حصل على عدة مئات من الدولارات كل شهر وكان بالإمكان أن يستمر هذا الأمر الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول وآخر عميل له وفقا للترتيب الأبجدي للحروف وحينئذا اكتف عدم وجود ما يسمي Zzwicke[1].

وهناك مثال آخر لموظف أمريكي يدعي E. Royce كان يعمل بإدارة ائتمان بمنشأة تجارية ضخمة (تجارة الفواكه والخضار بالجملة) حيث لجأ إلى تقنية Salami لاستقطاع مبالغ زهيدة وعلى فترات زمنية طويلة ومتباينة من خلال الصفقات العديدة التي أبرمتها المنشأة مع المنتجين وموزعي التجزئة. حيث أعد Royce برنامج للإدارة المعلوماتية وعلى نحو يسمح بإدارة منتظمة لحسابات المنشأة والتي تتضخم فيه فترات زمنية معينة ببعض الإيرادات ثم يقوم باستقطاع مبلغ زهيد كل شهر من هذه الإيرادات واستطاع Royce أن يحقق فائدة على قدر كبير من الأهمية من خلال هذه المبالغ الزهيدة وتمكن في خلال ست سنوات من اختلاس مليون واحد من الدولارات[2].

و- القنابل المنطقية : Bombe Logique

إذا أراد محتال أن يسرق سيارة مصفحة مليئة بالنقود، فهو لن يفعل ذلك يوم الأثنين أو الثلاثاء ولكن سيختار بالأحرى يوم الجمعة لأن السيارة

(1) راجع د. محمد سامي الشوا، سابق الإشارة إليه ص 78.

(2) انظر :

Linformatique aujourd lui dans le no special monde sep. 1982 .

ستكون عندئذ مليئة بالمال ويتطابق الموقف في مجال الإجرام المعلوماتي وخصوصا بالنسبة لأفعال الغش المبرمجة على الحاسبات الآلية ولكن يجب توافر بعض الشروط والتي يمكن اكتشافها بصفة آلية حتى يمكن أن ينجح الاحتيال وعلى نحو مؤكد. ومن هنا تصبح القنبلة المنطقية وسيلة سهلة وجذابة.

والقنبلة المنطقية عبارة عن برنامج أو جزء من برنامج ينفذ في وقت محدد أو على فترات زمنية منتظمة ويتم وضعه داخل النظام المعلوماتي بهدف تحديد ظروف أو حالة محتويات النظام من أجل تسهيل تنفيذ عمل غير مشروع[1].

ويمكن على سبيل المثال إدخال تعليمات في برنامج نظام التشغيل (وهو البرنامج الذي يقوم بتحميل ذاكرة الحاسب بالبرامج المراد تنفيذها) وهو الذي ينفذ في كل مرة عمل جديد، وينصب البحث على عمل معين يمكن أن يكون محلا للاعتداء، كأن تسعي القنبلة المنطقية إلى البحث عن حرق معين وليكن (حرف الباء) في أي سجل يتضمن أمر بالدفع وعندما تكتشفه تتحرك متتالية منطقية sequence loghique تعمل على إزالة هذا الحرف من السجل[2].

والقنبلة الزمنية Bombe a retardement على عكس القنبلة المنطقية حيث تشير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة[3]. ويتم إدخالها في برنامج وتنفذ في جزء من الملي ثانية أو في بضع ثواني أو دقائق

(1) انظر في ذلك :

D. Parker, op. cit., p. 110.

(2) انظر في ذلك المرجع والمكان السابقان.

(3) وعبارة أخري فالقنابل الزمنية : هي تلك الفيروست التي تطلق في تاريخ محدد.
والقنابل المنطقية وهي تلك الفيروسات التي تطلق لشروط محددة.
راجع في ذلك :

Cr. Linda Volonino Cyber Terrorism. Op. cit.

وفقا للتحديد المطلوب ويمكن على سبيل المثال ضبطها لكي تنفجر بعد عامين في يوم 12 يونيو الساعة أثنين وخمس وأربعون دقيقة (12.45) عصرا لتحويل مبلغ من المال من حساب شخص معين تلاحظ في نفس اللحظة الذي يكون فيها مرتكب الجريمة متواجدا في البرازيل Riod Janeiro.

ومن أمثلة استخدام القنبلة المنطقية ما يلي :

1- قام مبرمج في ألمانيا الديمقراطية (قبل توحيدها) بزرع برنامج يحوي قنبلة زمنية في النظام المعلوماتى الخاص بالشركة التي يعمل بها وتم برمجة القنبلة بحيث تنفجر بعد عامين لتركه العمل بها وفي حوالي الساعة الثالثة ووفقا للتاريخ المحدد وكما سجل هذا الأخير في البرنامج، فإن الاستفهام الخاص بيوم وساعة وسند التنفيذ ظل مستمرا، وكان متأكدا من أن لحظة التدمير ستراعي بكل دقة. وبسبب طارئ أدي إلى انهيار النظام المعلوماتي الخاص بالشركة فإن أكثر من 300 طرفية ظلت لا تعمل لبضة أيام وكان من الصعب اكتشاف الفاعل نظرا للتفاوت في الزمن بين لحظة ارتكاب الفعل ولحظة تحقيق النتيجة[1].

2- تمكن أحد العاملين بإدارة المياه والطاقة في ولاية لوس انجلوس الأمريكية من وضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها مما أدي إلى تخريب هذا النظام عدة مرات[2].

3- استطاع خبير في نظم المعلومات في الدانمارك من وضع قنبلة منطقية في نظام إحدى الحاسبات الآلية الأمر الذي ترتب عليه محو أكثر من

(1) Hartmann, La criminalité informatique et sa repression par les reformes penales en Allemagne, Droit de l'informatique 1985-6-annex p. 11.

(2) انظر د. هشام رستم، سابق الإشارة إليه ص 160 .

100 برنامج. وقد تم أيضا محو النسخ الاحتياطية عند تشغيلها نظرا لانتقال آثار القنبلة إليه وتم ضبط المجرم وحكم عليه بالحبس لمدة سبعة شهور.

ك - فيروس الحب:

تعاني شبكات الكمبيوتر من الإرهاب عبر الإنترنت بشكل متزايد وذلك على شكل محاولات متعددة لزرع فيروسات ببرامج الكمبيوتر عبر ملحقات البريد الإلكتروني.

ومؤخرا فقد سبب فيروس الحب المدمر خسائر مدمرة لا تزال شركات عديدة تعاني منها، وأسلوب فيروس الحب في الهجوم يعتمد على إرسال رسالة مغزية شكلا ومضمونا لحث المتلقين على فتحها.

وفيروس الحب هو نوع من الفيروس المعروف بـ "حصان طروادة" أو دودة البريد الإلكتروني وستظهر أنواع جديدة من هذا الفيروس قاردة على تهديد ملفات المعلومات الخاصة بالشركات التجارية الكبرى.

الطريقة التي يعمل بها فيروس الحب وما شابهه من فيروسات :

- يصل فيروس الحب على شكل رسالة إلكترونية عادية لها ملحق يسمي "رسالة حب لك نص" هذا في حال تعطيل خاصية الإظهار الكاملة لنهايات الملفات حيث أن الجزء الأخير من اسم الملف هو "في.بي.اس" وفي هذه الحالة يتنكر الفيروس في شكل رسالة بريدية نصية آمنة تماما، بينما في الحقيقة تستطيع هذه الرسالة تنفيذ أوامر برمجة كمبيوترية مدمرة.

بعد فتح الملف المصاب بالفيروس، يقوم الفيروس بتنفيذ خمسة عمليات مدمرة :

1- يقوم بنسخ نفسه للعديد من الملفات الأخرى، بما يضاعف قدرته على الانتشار.

2- يقوم بتعديل ملف التسجيل الخاص بالكمبيوتر المصاب حتى يمكنه إعادة تنفيذ البرنامج الخاص بالفيروس في كل مرة يتم فيها تشغيل الحاسوب، وكما يقوم ايضا بتشغيل خاصية سرقة كلمة سر من موقع للإنترنت.

3- يقوم بتحديد صفحة قياسية جديدة لبرنامج مايكروسوفت انترنت إكسبلورر.

4- يقوم بإرسال رسالة بريد إلكتروني لكل مستخدمي الكمبيوتر المصاب وكذلك كافة قوائم التوزيع الموجودة بسجل العناوين الإلكترونية الخاص ببرنامج "أوت لوك".

5- يقوم بإصابة كافة سائقات البحث بما في ذلك تلك الخاصة بالشبكة المستخدمة بالشركة والمرتبطة بالجهاز المصاب ويقوم الفيروس إما بحذف الملفات أو إخفائها ويستبدلها بنسخ منه.



المبحث الرابع

انتشار الفيروسات المعلوماتية وأساليب الوقاية منها

- العوامل المؤثرة في انتشار الفيروسات المعلوماتية[1]:

أصبحت شبكة الإنترنت المكان الأمثل لارتكاب جرائم الاحتيال والنهب، بما تتمتع به من تكلفة تركيب منخفضة بالإضافة لإمكانية التعمية الكاملة على الشخصية، وإمكانية الوصول لملايين الضحايا المحتملين عبر أنحاء العالم، فبوسع المجرمين الاختفاء في بلاد بعيدة وانتحال هوية آخرين أو حتى استخدام أدوات ذات تقنية عالية مثل الكتابة المشفرة "الهواتف الخليوية، برامج النشر الصحفي، وبرامج اللوغاريتمات الرياضية التي يمكنها تكوين أرقام عاملة لبطاقات الائتمان.

ويوضح Louis J. freeh مدير مكتب المباحث الفيدرالية الأمريكي أن الانترنت هي وسط ممتاز لالتقاط الضحايا كما أنها توفر بيئة لا يستطيع فيها الضحايا أن يتحدثوا أو يروا المحتالين، فبوسع أي شخص يحتمي بخصوصية جدران منزله أن يخلق وسيلة احتيال شديدة القناع عبر الإنترنت.

أما Arthur Levitt رئيس قسم مكافحة الجرائم الإلكترونية "سك" فيقول: يمكن بنقرة ماوس إيصال رسالة بريد إلكتروني جماعية غير مخصصة (spam) للمستثمرين بطريقة أسهل وأرخص من تلك المكالمات الباردة التى تجرى بشكل تقليدي كما أن استخدام الوسيلة الإلكترونية يضفي مسحة من المصداقية على ما يستخدمه المحتال من أدوات حيث بإمكان أي شخص يمتلك جهاز كمبيوتر منزلي ومعرفة بنظم الرسم الإلكتروني (graphies) أن يصمم

---

(1) راجع في ذلك :

REPIRT 5

- The first conference on computer forensics & Digital Discovery Tools & Techniques October 21st – 23rd , 2000.

موقعا جذابا - على أقصى درجة من الحرفية - يضاهي موقع شركة "فورشت 500" على الإنترنت. وفي نفس الوقت يقف تطبيق القانون عاجزا نتيجة لميراث ثقيل من القوانين الصادرة في عهد ما قبل الإنترنت، تلك القوانين التي تضع قيودا على عملية التحري والحدود الجغرافية لسلطة الضبط القضائي.

وحتى الآن فقد تم ضبط القليل من محتالي الإنترنت بينما يخضع عدد أقل منهم لعقوبات شديدة، ويضع وصول الإنترنت لكافة أنحاء الكوكب مؤسسات تطبيق القانون المحلية في حرج، نظرا أنشأت لحماية الحدود الجغرافية للمدينة أو للمقاطعة أو الدولة، بدون أن يكون لديها لا الإمكانات ولا الخبرات التي تمكنها من مواجهة الجرائم المعقدة للاحتيال عبر الإنترنت.

وتعاني الوكالات القومية المتخصصة في مواجهة جرائم الاحتيال الإلكتروني من الإحباط نتيجة الميراث الثقيل من التشريعات التي سنت قبل عهد الإنترنت، ومن شهر هذه الوكالات الشرطة السرية لوزارة الخزانة، والمفوضية التجارية الفيدرالية (إف. تي. سي) F.T.C.، وقسم التفتيش البريدي الأمريكي (يو، أس، بي، اس) U.S.B.S. ومكتب المباحث الفيدرالية الأمريكي، وقسم مكافحة الجرائم الإلكترونية (سك) Securities & Exchange Commission ، ويعود هذا الإحباط إلى القيود المفروضة على عمليات التحقيق والحدود الجغرافية لسلطة التحقيق، وعلى سبيل المثال، فقد تشابكت خطوط التحقيق بقضية نصب إلكتروني كبري حينما مارس محتالوا الإنترنت - الذين استهدفوا نشاطات تجارية أمريكية كبري - نشاطاتهم من خارج الحدود.

ففي هذه الحالة من المحتمل أن يكونوا بمنأى عن الملاحقة القضائية حيث أنهم لا ينتهكون أي قوانين فلا وجود لأي قوانين معمول بها حيث يعملون.

وبوسع سلطات الجمارك الأمريكية - بما تتمتع به من سلطة الضبطية القضائية على نطاق قومي - أن توضح عددا من الحالات الناجحة للتنسيق مع سلطات الضبطية القضائية لدول أخري.

ففي إحدى الحالات تم تنظيم غارات متزامنة في إثني عشر دولة تضم الولايات المتحدة و 10 دول من أوروبا الغربية بالإضافة لاستراليا، ومع ذلك يعترف Raymond W. Kelly المفوض العام لمفوضية الجمارك الأمريكية أنه لا يوجد سوي إجماع ضئيل على مسوي دول الكوكب حول ما هي الأنشطة التي يمكن وصفها بـ "الإجرامية" وتلك التي لا تنطبق عليها هذه الصفة.

- انعقد في مايو 2000 أول مؤتمر لـ "مجموعة الثمانية" حول المسائل المتعلقة بجرائم الإنترنت هذا ولا تزال الخطوط العامة لسياسة الاتحاد الأوروبي حول الجرائم الإلكترونية في طور الإعداد.
- القبض على المحتال ومع ذلك فلا عقوبة.

قد ينأي المحققون بأنفسهم عن إقامة الدعوى في قضايا الاحتيال المالي المعقدة في ظل نظام جنائي يميل لمقاضاة مجرمي الشوارع، حيث أن المحققون ليست لديهم المصادر التي تمكنهم من بناء دعوى يمكن لهيئة المحلفين متابعتها، أو أن المبالغ الخاصة بالقضية قليلة جدا أو لقلة لعدد بقائمة الضحايا.

ويدرك العديد من المحتالين الحدود المالية التي تستلزم تدخلا من سلطات فرض القانون لذا يبقون حدود عمليات احتيالهم أقل من هذه الحدود وطبقا لجريدة "نيويورك تايمز" فإنه بينما وصلت نسبة القبض على مرتكبي الجرائم من ذوي الياقات البيضاء إلى ذروة معدلاتها منذ خمسة أعوام مضت. فإن نسبة الجرائم التي يرتكبها ذوي الياقات البيضاء قد ارتفعت (في النظم الاقتصادية القديمة والحديثة) بنسبة تتراوح بين 10% و20% خلال

الخمسة أعوام الأخيرة. ويحتج Skolook المفوض العام لشركة "أنديانا" للمستندات المالية ورئيس اتحاد المتعاملين في السندات المالية بأمريكا الشمالية (إن-إيه_إس-إيه-إيه) N.A.S.A.A. على أن جرائم ذوي الياقات البيضاء لا ينظر إليها بشكل جدي نظرا لكونها معقمة وتخلو من سقمك الدماء ولكونها جرائم فنية فإذا ما تم القبض على محتالي المستندات المالية. فإنهم يواجهون قيما إدارية أو مدنية وليس الملاحقة الجنائية ويضيف Skolook الملاحظة التالية إذا سرق أحدهم سيارتك فسوف يلقي به في السجن أما إذا سرق محتال - إلكترونيا- أموال والديك الذين يحتاجون إليها عند تقاعدهما عن العمل فربما يدفع غرامة فعلته هذا ليس عدلا.

يعتقد الكثير من النقاد، يؤيدهم في ذلك مطبقي القانون أنه على الرغم من زيادة الإجراءات الأمنية الجديدة لمواجهة جرائم الإنترنت فإن المجرمين سيتمكنون من زيادة حجم جرائمهم ذات المستوي التقني المرتفع لفترة من الزمن.

وقد تمثل أحد ردود الأفعال على موجة الجرائم الرقمية في جعل مشاركة المعلومات والتعاون بين الشركات يتم بشكل رسمي وبهذا يمكن التأكد من هذه المعلومات، فعلي سبيل المثال تطبق F.T.C. سياسة أيام تطبيق القانون على التجول عبر الشبكة وخلال تلك الأيام تنسق الوكالات الفيدرالية فيما بينها عملية مراقبة الشبكة.

ويشكل مركز حماية البنية الأساسية القومي N.J.B.C. الذي أنشأ عام 1998 للكشف عن مواجهة الهجمات الإلكترونية على البنية التحتية القومية الحيوية ومركز I.F.C.C. الجديد والذي بدأ نشاطه هذا الربيع لجمع وتحليل الاستخبارات الخاصة بجرائم الاحتيال عبر الإنترنت أمثلة على التسهيلات المقدمة من وبين الوكالات المختلفة العاملة تحت حماية مكتب المباحث الفيدرالي الأمريكي كما تبذل جهود متناسقة لتغيير القوانين التي تشكل عائقا

لملاحقة مجرمي الإنترنت. لذا تعمل وزارة العدل على إصدار تشريعات جديدة لتحديث القوانين التي تحكم عمليات التحري والإدعاء في مجال جرائم الإنترنت، ويعلق مدير مكتب المباحث الأمريكية الفيدرالية السيد Freeh قائلا لقد تطورت مشكلة جرائم الإنترنت بشكل سريع أعجز القوانين القائمة عن ملاحقة التغير التقني ومن بين الأمثلة التي أوردها تحت القوانين المعمول بها حاليا فإن المحكمة الفيدرالية تستطيع إصدار الأمر بتتبع الاتصالات المجراة فقط داخل منطقة عملها وذلك لتزويد سلطات تطبيق القانون بمعلومات المراقبة، ولا نحتاج هنا للقول بأن عملية تتبع اتصال واحد قد يكون مضيعة للوقت والموارد وبهذه الطريقة تتم عملية إعاقة أو إحالة أمد التحقيقات في مثل هذه الحالات التي تتصل فيها سلطات فرض القانون بمقدم خدمة الاتصالات بعد أن يكون قد تخلص من المعلومات الضرورية للتحقيق.

حدود تطبيق القانون :

بالطبع فهناك العديد من نقاط الاستفهام حول تطبيق القانون الموضوع لحماية الحقوق الدستورية للأفراد فالمدافعين عن حقوق الفرد الساعين لرؤية هذه الحقوق مطبقة في الحقبة الإلكترونية يخرجون باعتراضات جديدة لبعض المحاولات لتوسيع السلطات الشرطية في مجال الإنترنت.

فعلي سبيل المثال : فإن مركز المعلومات الإلكترونية الخصوصية (إيبك) وإتحاد الحد فوق المدنية الأمريكية A.C.L.U. ومنظمة الحدود الإلكترونية E.F.F. قد رفعوا دعوى بالمحكمة في نوفمبر 1999 لمنع تنفيذ القواعد الفيدرالية الجديدة في مجال الاتصالات F.C.C. حيث أن هذه القواعد ستمكن مكتب المباحث الفيدرالية الأمريكي من فرض تصميم البنية الأساسية لنظام الاتصالات القومي، فطبقا لقانون مساعدة نظم الاتصالات لتطبيق القانون (كاليا) والذي سن عام 1994 فيتعين على شركات الاتصالات

تصميم أنظمتها بما يتوافق مع المستويات الفنية للمباحث الفيدرالية الأمريكية وذلك لتسهيل عمليات المراقبة الإلكترونية، ولكن يدفع المعارضون بأن أحكام القواعد الفيدرالية الجديدة في مجال الاتصالات F.C.C. تعطي وكالات فرض القانون سلطات أكبر من تلك التي منحها لهم الكونجرس، ولم تقف جماعات لحقوق الشخصية بمفردها في هذه المعركة فقد رفع اتحاد الاتصالات واتحاد صناعة الهواتف الخلوية قضايا مماثلة لنقض أحكام القواعد الفيدرالية الجديدة في مجال الاتصالات F.C.C. وقانون مساعدة نظم الاتصالات لتطبيق القانون (كاليا).

لا يستطيع القطاع الخاص الاعتماد بصورة كلية على تطبيق مواد القانون لحماية مصالحه على الجبهة الرقمية وعلى الرغم من أن وسائل تطبيق القانون تكتسب أدوات جديدة تمكنها من حراسة القضاء الإلكتروني فإن العملية تستلزم مجالا عميقا وطويل الأمد حول أفضل الطرق لإزالة العوائق التي تخدم أساسا المجرمين، بينما تضع قيودا ثقيلة على سلطة الحكومة على التدخل في الحياة الشخصية للأفراد. وكما قال William M. Daley وزير التجارة الأمريكي تحشد من خبراء تكنولوجيا المعلومات اجتمع هذا الربيع "هذه هي أول مرة في التاريخ الأمريكي لا تستطيع الحكومة بمفردها حماية البنية الأساسية للدولة فلا نستطيع تأمين قوة شرطية كبيرة بما فيه الكفاية لحماية كافة أصول المعلومات الرئيسية لصناعتنا، بل لن ترغبوا أنتم في أن نقوم بذلك".

- أساليب الوقاية من الفيروسات المعلوماتية:

تتعدد أساليب الوقاية من الفيروسات المعلوماتية وذلك على النحو التالي :

أولا : الاحتياطات العامة لمواجهة الفيروسات المعلوماتية [1]

يجب تحميل برنامج مضاد للفيروسات داخل كافة الأنظمة المعرضة لخطر الإصابة بها ويمكن الأخذ بالاحتياطات التالية للحد من سرقة انتشار الفيروسات:

1- أن يتم إدخال البرامج المحملة عن طريق الإنترنت من المواقع الموثوق فيها فقط.
2- ألا يتم استخدام أي من الأقراص المرنة داخل الكمبيوتر ما لم يجر عليه فحص دقيق للتأكد من خلوه من الفيروسات.
3- وقف عمل وحدة (الماكرو) كلما أمكن ذلك.
4- يمكن تطعيم الأقراص المرنة ضد الفيروسات التي تصيب قطاع التحميل.
5- الإبقاء على شريط الحماية الموجود بالبرامج الجديدة المسجلة على الأقراص المرنة.
6- يجب على مهندسي الكمبيوتر الذين ينتقلون من شبكة إلى أخرى كفالة حماية الأقراص المرنة التي يستخدمونها.

ثانيا : بعض الاحتياطات الخاصة لمواجهة الفيروسات المعلوماتية

1- برنامج كمبيوتر يقضي على فيروسات الماكرو والفيروسات الخاصة بلغة لنص الحساس في البريد الإلكتروني :

أطلقت شركة "جي.إف.آي." J.F.I. اليوم برنامجها الرئيسي لحماية البريد الإلكتروني تحت اسم "ميل اسنشيالز اكستينج إس أم تي بي 3.5" وهو برنامج لفحص محتوي الرسائل الإلكترونية بالإضافة لكونه برنامج

---

(1) راجع في ذلك :

Dr : Linda Volonino Cyber Jerrorism op. cit.

مضاد للفيروسات، ويمكن لهذا البرنامج حاليا أن يحمي أجهزة تخزين وإرسال البريد الإلكتروني (الأجهزة الخادمة) ضد جميع فيروسات الماكرو (الماكرو هو مجموعة أوامر تنفيذية فرعية داخل برنامج آخر) وفيروسات لغة النص الحساس في البريد الإلكتروني حاليا ومستقبلا ويعزز هذا الأسلوب من تأمين أجهزة تخزين وإرسال البريد الإلكتروني الرئيسية (الأجهزة الخادمة) مع التأكد من حماية المستخدمين ضد كافة الفيروسات المستقبلية للماكرو ولغة النص الحساس في البريد الإلكتروني، حتى قبل أن يصدر منتجو برامج محاربة الفيروسات أي تحديث لقائمة فيروسات برامجهم.

وقد صرح السيد/ جاليا – منتج هذا البرنامج- بأن برنامج ميل اسنشيالز 3.5 يوفر حماية شاملة لبرامج البريد الإلكتروني، حيث بإمكانه حاليا محو أي ماكرو وأي كتابة بلغة النص الحساس من برنامج "ورد" بطريقة آلية، فإذا ما وجد هذا البرنامج أي نص ملحق يحتوي على ماكرو، فإنه يقوم أوتوماتيكيا بمحو الماكرو فورا وسيتم إرسال الوثيقة للمرسل إليه بدون هذا الماكرو الخطير وبهذا يتم تأمين الوثيقة كليا، كما أوضح أيضا أن الفيروسات سيئة السمعة، مثل "ميليسا" الذي انطلق العام الماضي وفيروس "ريزومي الذي انطلق هذا العام 2000 يعتبران مثالين شهيرين على فيروسات الماكرو كما أوضح السيد/ جاليا أيضا أن دخول لغة النص الحساس في البريد الإلكتروني قد مكن مخترقي أنظمة الكمبيوتر وواضعي برامج الفيروسات أن يطلقوا سلسلة من الأوامر عبر تضمنيها في رسالة إلكترونية تستخدم هذه اللغة ويمكن هنا لبرنامج "ميل اسنشيالز" توفير حماية كاملة لمستخدميه في مثل هذه المواقف، حيث يقوم باكتشاف مثل هذه الأوامر ومحوها بشكل آلي، ومع ذلك يتم إرسال الرسالة للمرسل إليه، ولكن مع تعطيل كافة الأوامر المكتوبة بلغة النص الحساس وبهذا يتم تأمين الرسالة.

ويفضل هذه الإمكانات الإبداعية الأمنية ينعمن مستخدمي برنامج "ميل اسنشيالز" بتأمين أجهزة حواسبهم، حتى ضد كافة فيروسات الماكرو وفيروسات لغة النصوص الحساسة التي ستنطلق مستقبلا، وذلك قبل أن يطرح منتجو برامج محاربة الفيروسات إصدارات تحديث قائمة الفيروسات الخاصة ببرامجهم، وبالإضافة إلى ذلك يأمن مستخدموا البرنامج شر الهجمات عبر البريد الإلكتروني، وخصوصا تلك الهجمات الشاملة الموجهة تحديدا ضد الشبكة والتي لا توفر برامج محاربة الكمبيوتر أي دفاع ضدها.

كما يمكن لبرنامج "ميل اسنشيالز" أيضا أن يقوم باعتراض أي رسائل إلكترونية أو أي من ملحقاتها تستخدم أي من لغات البرمجة مثل في. بي V.B (التي استخدمها فيروس الحب) أو لغة لنصوص الخاصة ببرنامج "ويندوز" أو لغة "جافا" وذلك على مستوي أجهزة تخزين وإرسال الرسائل الإلكترونية الرئيسية (الأجهزة الخادمة) حيث أن هذا البرنامج يعمل كبوابة أمن لفحص محتوي الرسائل قبل وصولها للجهاز الخادم، هكذا فإنها تقوم بعمل "الجدار الناري" بالنسبة لبرنامج البريد الإلكتروني، حيث تقوم بعزل كل الرسائل المشكوك بها قبل وصولها لمستخدمي البريد الإلكتروني وإصابتهم بأذي.

ويوفر الإصدار الأحدث من هذا البرنامج مزايا إضافية لفحص محتوي الرسائل مثل القدرة الآلية على محو ملحقات الرسالة الإلكترونية، ويقدم برنامج "ميل اسنشيالز" المزايا التالية:

- تنقية واختبار محتوي الرسائل.
- منع تسرب المعلومات الشخصية.
- فحص كافة الرسائل ضد الفيروسات.
- إجرائيات متقدمة لمنع التعرض للإغراق بالبريد الإلكتروني.
- إخطارات عدم المسئولية : حيث بإمكانك أن تضيف إخطار بعدم المسئولية مع بريد إلكتروني ترسله.

- إدارة البريد الإلكتروني : التقارير، حفظ وأرشفة كافة الرسائل، إمكانية تحميل بروتوكول 3 للبريد الإلكتروني، ردود آلية عبر الجهاز الخادم.

2- برامج كمبيوتر توفر الحماية ضد الثغرات الأمنية بالبريد الإلكتروني :

- البرامج التقليدية للحماية ضد الفيروسات لا حول لها ولا قوة أمام هذا التهديد الجديد :

أعلنت شركة "جي.إف.آي" J.F.I. والتي تعمل في مجال برامج الكمبيوتر الخاصة بتأمين البريد الإلكتروني ومحاربة الفيروسات، عن أنها توفر حلا ضد الجيل الجديد من فيروسات البريد الإلكتروني التي يمكن أن تنتشر حتى لو لم يقم المستخدم بفتح ملحقات الرسالة حيث يمكن استخدام برنامج شركة J.F.I. لفحص محتوي الرسالة الإلكترونية، والذي أطلقت عليه اسم "ميل اسنشيالز" للحماية ضد هذا التهديد الجديد والخطير على مستوي الجهاز الخادم للبريد الإلكتروني وقد أوضح رئيس مجلس إدارة الشركة بأنه "وفقا لتوقعات خبراء أمن الحاسوب، فإن كل جيل جديد من فيروسات البريد الإلكتروني يصبح أخطر وأكثر إيذاء مما يحتم ضرورة قيام المؤسسات بإحكام إجراءات الأمن الخاصة بالبريد الإلكتروني، وفي الوقت الحاضر فإن نقطة ضعف جديدة يمكن استغلالها لإرسال فيروسات خاصة بالبريد الإلكتروني حتى تبدأ نشاطها.

وكنتيجة لنقطة الضعف هذه والموجودة بإصدارات شركة مايكروسوفت فإن أجهزة الكمبيوتر الشخصية التي تستخدم برنامج التصفح "إنترنت إكسبلورر" الإصدار الخام و/أو برنامج "مايكروسوفت أوفيس 2000" عرضة لهجمات الفيروسات التي تستخدم لغة النص الحساس الموجودة ببرامج البريد الإلكتروني حتى لو لم يفتح المتلقي أي ملحقات مع الرسالة التي وصلت.

ومشكلة تأمين البريد الإلكتروني هذه ناجمة عن ثغرة في عملية برمجة معيار التحكم النشط "إكس" الخاص ببرنامج "إنترنت إكسبلورر" ويسمي "اسكريبت لت تايب ليب" ولسوء الحظ ونظرا لسهولة استغلال هذه الثغرة فإن الوقت سانح لحدث تدميري هائل على الأقل يمكن مقارنته بتأثير فيروس الحب الذي ضرب ضربته في مايو 2000.

وليس بوسع البرامج التقليدية للحماية ضد الفيروسات أن تحمي ضد هذه الأنواع من الفيروسات إلا أن برنامج "ميل اسنشيالز" يمكنه أيضا أن يقوم باعتراض أي رسائل إلكترونية أو أي من ملحقاتها تستخدم أي من ملفات البرمجة مثل V.B. (في. بي) التي استخدمها فيروس الحب أو لغة النصوص الخاصة ببرنامج "ويندوز" أو لغة سجافا" وذلك على مستوي أجهزة تخزين وإرسال الرسائل الإلكترونية الرئيسية (الأجهزة الخادمة)، حيث أن هذا البرنامج يعمل كبوابة أمن لفحص محتوي الرسائل قبل وصولها للجهاز الخادم، فإنها تقوم بعمل "الجدار الناري" بالنسبة لبرنامج البريد الإلكتروني، حيث تقوم بعزل كل الرسائل المشكوك بها قبل وصولها لمستخدمي البريد الإلكتروني وإصابتهم بأذي.

وينصح مستخدمي برامج "إنترنت إكسبلورر" و "أوت لوك" بمراجعة الموقع المؤمن لشركة مايكروسوفت على الإنترنت للحصول على وسيلة مواجهة هذه الثغرة كما يتعين على مشغلي الشبكات تركيب برنامج يعمل كنقطة تفتيش أمني على محتوي رسائل البريد الإلكتروني، ويكون قادرا على كشف مل هذا الفيروس للتأكد من عدم انتقال مثل هذه الفيروسات لأجهزة تخزين وإرسال البريد الإلكتروني (الأجهزة الخادمة).

3- شركة J.F.I. (جي. إف. آي) تطلق برنامجها لكشف مخترقي كلمات السر "باس ورد سنيفر" للاستخدام مع برنامج "لانجارد".

"لانجارد" ليست حاطا ناريا شخصيا، بل هو برنامج للتحكم في الدخول إلى وكشف متسللي شبكة الإنترنت وهي مناسبة للاستخدام مع الشبكات،

ويتطلب برنامج "لانجارد" نظام تشغيل ويندوز إن تي 2000. ويكشف برنامج "لانجارد" متلصصي وسارقي كلمات السر على الشبكة ويسمح لإدارة الشبكة باتخاذ ما يلزم من إجراءات ضدهم.

ويشتمل برنامج "لانجارد" للتحكم في الدخول للشبكات والإنترنت حاليا على برنامج لكشف متلصصي كلمات السر وتمنع هذه الميزة الإضافية مستخدمي البرنامج تأمينا أفضل لشبكاتهم حيث أنها تتيح لبرنامج "لانجارد" الكشف عن أي جهاز كمبيوتر على الشبكة مزود ببرامج الكشف عن كلمات السر حيث يمثل مخترقي كلمات السر خطرا أمنيا داهما إذ بإمكانهم سرقة كلمات السر الخاصة بشبكة معلوماتك.

ويمكن لمنظمي الشبكة – بواسطة لانجارد- تحليل المعلومات المنقولة عبر الشبكة والكشف عن بعد أي جهاز كمبيوتر على الشبكة في حالة تلصص "أي في حالة تمكنه من رؤية المعلومات المنقولة عبر الشبكة وليس فقط المعلومات المرسلة إليه" ويتيح لك برنامج لانجارد الاستمرار في مراقبة الشبكة ومسحها لمعرفة الأخطار الأمنية المحتملة.

فعلي سبيل المثال يتيح البرنامج لمشغلي الشبكة معرفة أي من مستخدمي الشبكة يدخلون على مواقع معينة بأجهزة الكمبيوتر ويعلن رئيس لانجارد عن برنامج لانجارد قائلا "تسمح ميزة برنامج لانجارد، بالكشف عن متلصصي كلمات السر لمديري شبكات الكمبيوتر الكشف عن أولئك الذين يستخدمون برامج الكشف عن كلمات السر على الشبكة، واتخاذ الإجراءات التصحيحية اللازمة، "فلانجارد" وهو أداة أمنية لا غني عنها لضمان أمن شبكات الكمبيوتر، حيث يجب استخدامها بالاشتراك مع حائط ناري فهناك العديد من برامج اختراق وكشف كلمات السر التي توزع مجانا على شبكة الإنترنت، لذا لا تستطيع المنظمات والشركات التجارية أن تقف بلا دفاع ضد سرقة كلمات السر.

ويعمل برنامج لانجارد باستخدام تقنية ثورية للتجسس تسمح له بأن يدخل ويستقر داخل أي جهاز كمبيوتر بالشبكة. كما أن البرنامج يتأكد من الاستخدام البناء للانترنت كما يشتمل على ميزات ثورية تستطيع منع البحث عن كلمات وعبارات معينة على الإنترنت. **ويشتمل برنامج "فلانجارد" على المميزات التالية :**

- يحمي ضد سوء استخدام شبكة الإنترنت.
- يمنع الدخول على مواقع معينة على شبكة الإنترنت.
- يمنع البحث عن والدخول إلى مواقع معينة ذات محتوي خاص على الإنترنت.
- يمنع إصدار تقارير حول استخدام الإنترنت.
- يوفر تداخل أمني ممتد.
- لا يستلزم إعادة توصيف الشبكة.
- لا يؤثر على الأداء.
- لا يستلزم توصيفا خاص من قبل المستخدم.
- يراقب الشبكة ككل.

وعلى أية حال، لم يعد الشخص المتعامل مع الحاسب الآلى بحاجة لبرنامج مكافحة الفيروسات؛ وذلك نظرا لأن معظم شركات إنتاج هذه البرامج، بدأت تخرص على توفير العلاج ضد أى فيروس يكون قد ضرب ضربته الضارة بالفعل، وذلك إما باستخدام برنامج لفحص محتوي رسائل البريد الإلكتروني فيمكن منع وقوع الضرر قبل حدوثه، كما يمكن لبرنامج الحماية الذي يفحص مضمون الرسائل الإلكترونية، اعتراض أي رسائل أو ملحقاتها تعتمد على لغة برمجة مثل نصوص لغة "فيجوال بيسك" أو أية ملفات أخري ذات أوامر تنفيذية وذلك على مستوي الجهاز الرئيسي (الخادم).

ومن المؤكد أن الطريقة الوحيدة للحصول على تأمين كامل ضد فيروس الحب وكافة النسخ المعدلة منه هو اعتراض وإيقاف كافة رسائل البريد الإلكتروني التي تحتوي نصوصا خاصة بالبرمجة على مستوي الجهاز الرئيسي (الخادم). وذلك بعزل هذه الرسائل وهذه هي أكثر الطرق أمانا لمنع الإصابة بهذه الفيروسات.

وبعد هذا الحديث المطول عن الفيروسات يثار تساؤل مهم مؤداه: كيف تمنع المجرمين من الولوج إلى حاسوبك، وكيف تتعرف على أصحاب النوايا الإجرامية على شبكة النت فتأمن شرهم؟

الحقيقة التى يجب أن نشير إليها أن المسألة ليست بالسهولة التي نتصورها، فهذا أمر صعب وهو أحد أسباب خطورة جرائم الإنترنت، حسبما يؤكد المتخصصون؛ ذلك أن المخربين يظهرون بصورة الناصح، أو المرشد مما يتسبب في خداع الضحية، كما أنه لا يمكن التعرف على هوية المخرب، فقد يظهر بهوية مزيفة ويمكن أن يكون التخريب على شكل برامج يتم تحميلها من الإنترنت وتحوي فيروسات، كما يمكن أن تكون على شكل مرفقات مع البريد الإلكتروني.

الواقع أن المخربين على الإنترنت يختلفون من جهة الخطورة؛ فمنهم المستخدم العادي الذي يستطيع الوصول لأغراض تخريبية، ومنهم الهاوي الذي يتعلم بعض المهارات على حساب الآخرين، ومنهم المحترف الذي يقصد التخريب، ومنهم العصابات المنظمة. ولهذا فمن أنجع الوسائل أن يتم التعامل مع الأشخاص على الإنترنت بحذر شديد، وألا يتعامل إلا مع أشخاص أو مواقع معروفة، بحيث لا يتم تحميل ملفات إلا من المواقع الموثوقة، ويمكن الاستفادة من تقنية التوقيع الرقمي والتي تعطى للمواقع عبر شركات كثيرة، حيث أن المواقع المعروفة لها توقيعات رقمية معترف بها. وهذه التقنية تدعمها برامج تشغيل الحاسبات المنتشرة في العالم مثل نظام

التشغيل ويندوز من شركة مايكروسوفت، ولهذا يتم تحذيرك إذا كان الموقع غير معروف (ليس له توقيع رقمي معروف أو معترف به)، وأيضا ينبغي التعامل بحذر مع رسائل البريد الإلكتروني بعدم فتح أي بريد يحوي مرفقات حتى لو كان من شخص يعرفه، إلا إذا كان المستخدم يتوقع وصول ذلك البريد، وذلك لاحتمال احتوائها على فيروسات أو ملفات تجسس.



الفصل الثالث

الجريمة الالكترونية فى مصر والدول العربية

يتناول هذا الفصل الجريمة الالكترونية فى مصر والدول العربية عبر ثلاثة مباحث تناول المبحث الأول منها الجريمة الإلكترونية فى مصر، فيما تحدث المبحث الثانى عن تنامى جرائم المعلوماتية والانترنت فى الدول العربية وآليات مواجهتها، وأخيرا ركز المبحث الثالث على إشكالية القصور التشريعى ونمط تعاطى القضاء العربى مع جرائم المعلوماتية.



المبحث الأول

الجريمة الإلكترونية فى مصر وأساليب مكافحتها

نتناول فى هذا المبحث انتشار جرائم الانترنت فى مصر ثم الآليات التى قررتها مصر لمواجهة الجرائم الالكترونية وأخيرا موقف القضاء المصرى من الجرائم الإلكترونية وضرورات إنشاء محكمة إلكترونية.

أولا: انتشار جرائم الانترنت فى مصر

دخلت خدمة الانترنت مصر عام 1993 علي يد مركز المعلومات ودعم اتخاذ القرار بالتعاون مع شبكة الجامعات المصرية ومع بداية عام 1997 بدأ المركز في خصخصة خدمات الانترنت في مصر وكانت البداية من خلال 16 شركة زادت الي 68 شركة في عام 2000 وانتهت الي 211 شركة هي اجمالي الشركات التي تقدم خدماتها في مجال الانترنت داخل مصر.

وقد بلغ عدد مستخدمي الانترنت في مصر في العام الاول لاستخدامه حوالى 75 ألف شخص ولكنه بعد تطبيق حملة حاسب لكل بيت وانخفاض أسعار خدمات الانترنت السريع وصل عدد مستخدمي الانترنت إلي ما يربو على خمسة ملايين و300 ألف مستخدم يحصلون علي خدماتهم من خلال 211 شركة تعمل في هذا المجال داخل حدود مصر.

وأكدت مصادر بالإدارة العامة للمعلومات والتوثيق بوزارة الداخلية المصرية على إن البعض استغل ما أتاحه العلم والتقدم التكنولوجي الحديث، استغلالا سيئا وبدأ في ارتكاب أعمال أو أفعال ترقى لمستوى الجريمة، وأصبحت تشكل هاجسا وتحديا للأجهزة الأمنية، وبات واضحا أن التهديد القادم شديد الخطورة في ظل ظروف دولية وإقليمية متشابكة، حيث جري الإعداد منذ أكثر من سنتين على تكوين وحدة مباحث جديدة تكون معنية بعملية رصد ومتابعة وضبط جميع الجرائم المستحدثة بجميع أشكالها

وأساليبها والتي يكون الكمبيوتر عنصرا في ارتكابها خاصة بعد أن بدأت هذه الجرائم تأخذ أشكالا وأبعادا دولية وعالمية جديدة وبشكل سريع.

ولعله من نافة القول الإشارة إلى أهم جرائم الالكترونية التى انتشرت فى مصر ومنها، جرائم استخدام بطاقات الائتمان المملوكة للغير، حيث يتم سرقتها واستخدامها في شراء سلع وخدمات من الخارج, ثم ظهرت بعض الجرائم الأخرى ذات الصلة بالكمبيوتر مثل جرائم الشبكات واختراقها والدخول على أجهزة الحاسب الآلي للغير وسرقة المعلومات التي تمثل سرية خاصة لبعض الأشخاص أو المؤسسات أو الشركات, كما ظهرت جرائم الإنترنت وقيام البعض بنشر مواقع تسيء لأشخاص آخرين أو تسيء لشكل ومظهر الدولة, ثم ظهرت جرائم عالمية أخرى يقوم بها بعض الهاكرز ومنها إطلاق الفيروسات والاختراقات، ومنها اختراق المواقع الرسمية أو الشخصية أو اختراق الأجهزة الشخصية وأنظمة شفرات الكمبيوتر للمؤسسات والأفراد، وجرائم التجسس الصناعي، وجرائم الأموال مثل السطو والاحتيال والنصب وسرقة بطاقات الائتمان والتزوير والجريمة المنظمة، وجرائم المخدرات وغسل الأموال، وجرائم الآداب وتجارة السلاح وجرائم الابتزاز الإلكتروني، وجرائم الغش الإلكتروني, بالإضافة إلى جرائم القرصنة وجرائم محتوى الإنترنت من المواقع الإباحية أو المعادية سواء دينيا أو سياسيا.

ويجب التأكيد على أن إدارة المعلومات والتوثيق بوزارة الداخلية تحتضن مجموعات عمل تعكف على متابعة شبكة الإنترنت على مدار اليوم لمراقبتها وفحص التعاملات والمعاملات التي تتم عليها من وإلى الخارج، وإذا ما ظهر أية مخالفات أو أعمال تمثل خروجا على القانون والشرعية أو تهديد أمن واستقرار الوطن يتم التدخل فورا بالتنسيق مع الأجهزة النوعية الأخرى.

ومما لا شك فيه أن التأثير المجتمعي الذي يحدثه التقدم التكنولوجي يحتاج إلي تنظيم قانوني، يضع إطارا للعلاقات التي تترتب علي استخدامه بما يكفل حماية الحقوق المترتبة علي هذا الاستعمال، ويحدد الواجبات تجاهها، فلابد للتقدم العلمي والتكنولوجي أن يواكبه تكيف في القواعد القانونية، إذ لا يجوز للقانون أن يقف صامتا مكتوف الأيدي حيال أساليب انتشار هذا التقدم، وحيال القيم التي يروجها.

ولا يقف دور القانون علي مجرد تنظيم العلاقات المترتبة علي التقدم التكنولوجي بل إنه يجب أن يحمي القيم التي تحيط باستخدام التكنولوجيا، ويحدد المسار الصحيح الذي يجب أن يسلكه التقدم التكنولوجي حتي لا يتخذه المجرمون أداة لتطوير وسائل إجرامهم، بل يكون علي العكس من ذلك وسيلة لمحاربة هذا الإجرام، وهو ما يوجب علي القانون أن تمتد نصوصه إلي الأنشطة الجديدة التي تفرزها التكنولوجيا حتي تحدد الجريمة في نصوص منضبطة واضحة، ولا يترك بحثها إلي نصوص قانون العقوبات التقليدي، التي قد تتسم بعدم اليقين القانوني أو لا تتسع لملاحقة الأنماط الجديدة من الإجرام.

ولعى أبة حال، استطاعت الشبكات الإلكترونية أن تغير من دور الدولة كأمة ومن سيادتها، لأنها أدت إلي انتشار فاعلين جدد عابرين للأوطان وإلي إنشاء نماذج دولية جديدة مثل مجتمع الإنترنت. وقد تتجاوز نتائج هذه الجرائم إلي وقوع جرائم أخري تهدد الحق في الحياة والسلامة البدنية، إذا ما أدي العبث في المعلومات إلي تغيير طريق العلاج أو تركيبة الدواء.

وحذر خبراء مصريون من أن جرائم الإنترنت قد تؤثر علي نطاق الخدمات الإلكترونية وقطاعات التنمية الاقتصادية، وتكنولوجيا المعلومات، خاصة أن مصر تطرح نفسها الآن كمركز متميز في مجال التكنولوجيا، الأمر الذي يتطلب إعادة هيكلة قطاع الاتصال، وتدعيم دور الدولة في حماية

المستخدمين تكنولوجيا الاتصالات، من خلال إجراءات تتميز بالشفافية الكاملة، خاصة أننا نواجه تحديات جديدة بما يعرف بالجريمة الإلكترونية، التي يجب مكافحتها، لتشجيع الاستثمار وحماية حقوق الملكية الفكرية، الأمر الذي يستلزم ألا يتم بمعزل عن الثوابت التشريعية والقانونية.

ومما يذكر أن التقدم التكنولوجي، قد أفرز أنماطا جديدة من الجريمة، وكذا من المجرمين، فكان للتقدم في العلوم المختلفة أثره علي نوعية الجرائم، ومن ثم فقد استغل المجرم المعلوماتى ثمرات هذه العلوم في تطويع المخترعات العلمية الحديثة لخدمة أهدافه الإجرامية، فالمشكلة الرئيسية لا تكمن في استغلال المجرمين الإنترنت، وإنما في عجز أجهزة العدالة عن ملاحقتهم، وعدم ملاحقة القانون لهم ومسايرة التكنولوجيا الجديدة لتشريعاته. فالقانون الجنائي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا الحديثة، لاسيما أن نصوص القانون الجنائي التقليدي وضعت في عصر لم يكن الإنترنت فيه قد ظهر، ولم تظهر بعد المشاكل القانونية الناشئة عن استخدامه، مما يفرض علي رجال القانون التدخل لمكافحة الجرائم الناشئة عن استخدام الإنترنت ومواجهة هذا النقص التشريعي، خاصة أنه لا يوجد لدينا نصوص خاصة بهذه الجرائم.

بالتالي، فقد تعولمت الجريمة وظهرت أنماط جديدة منها، وأصبحت الجريمة تنفذ عن بعد دون الحاجة إلي الفعل الفيزيقي بموضوع الجريمة مثل غسيل الأموال وتحويلها عبر الإنترنت وسرقة البنوك والحسابات التي لم تعد تتطلب السطو علي البنك في موقعه الفعلي، وإنما يمكن أن يكون ذلك إلكترونيا بتحويل أرصدة من الحسابات إلي حسابات أخري في دول أخري، فضلا عن ذلك فقد ظهرت جرائم الحاسب والجرائم المرتبطة به، وجرائم الملكية الفكرية وجرائم قرصنة الحاسب والتجسس العسكري والإلكتروني.. كل هذه الأنماط شكلت تحديا جديدا في تفسير الجريمة، وفي وسائل الوقاية

والمكافحة، لكننا نري أن البعض يتعامل مع هذا الخطر بسلبية وبطء شديدين لا يتماشيان مع خطورة وأهمية المرحلة، فهناك قصور واضح عربيا في مجال جرائم الإنترنت سواء من حيث أساليب التحقيق والرصد أو في مجال التوعية والتثقيف، وظهرت الحاجة إلي تثقيف القائمين بالضبط والخبراء وسلطات التحقيق علي التعامل وتفهم هذا النوع من المشاكل التي تحتاج إلي خبرات فنية عالية حتي تكون لديهم درجة من المعرفة الفنية تتناسب مع حجم المتغيرات والتطورات المتلاحقة في مجال جرائم تقنية المعلومات والإنترنت.

وهنا تبدور أهمية نشر الوعي المجتمعي بالمخاطر الاقتصادية والاجتماعية والثقافية، وغيرها الناجمة عن الاستخدامات غير الآمنة للإنترنت، وتكثيف التوعية عن الآثار السلبية الناتجة عن تلك الجرائم، لذلك تضافرت الجهود في مصر لكي يكون هناك دور أهلي تطوعي للقيام ضد مظاهر العدوان الإجرامي عبر الإنترنت عن طريق إنشاء الجمعيات والمراكز المهتمة بمكافحة الجرائم عبر الإنترنت.

ثانيا: التكييف القانونى للجرائم الالكترونية فى مصر وآليات مواجهتها

علي الرغم من هذا الكم الرهيب من الجرائم التي ترتكب علي شبكة الانترنت الا ان هناك فراغا تشريعيا في مواجهة هذه الجرائم التي مازالت تخضع لقانون العقوبات العادي الذي اصبح غير قادر علي مواجهة هذه النوعية من الجرائم المستحدثة التي تحتاج فى تكييفها إلى قانون محدد.

وعلي الرغم من انتشار هذه الجرائم في مصر فى ظل جهود الحكومة المصرية من أجل جذب الاستثمارات في مجال التكنولوجيا إلا ان هناك فراغا تشريعيا في هذا المجال خاصة في قضايا النشر الالكتروني وقوانين جرائم الانترنت الخاصة باقتحام النظم وغيرها، فالحقيقة أن مصر لا يوجد بها نظام قانوني خاص بجرائم المعلومات، إلا أن القانون المصري يجتهد

بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية.

وقد أرجع المتخصصون هذا الفراغ من أية عقوبات خاصة بجرائم الانترنت فى التشريع المصرى إلى حداثة هذا المجال الذي لم يتعد عمره سنوات قليلة وما يطبق حاليا علي جرائم الانترنت هو القانون التقليدى الذى يتم بموجبه تطبيق العقوبة على مرتكبى الجرائم العادية مثل جريمة السرقة، حيث يعاقب مرتكبها بالحبس مدة لاتقل عن 24 ساعة ولاتزيد علي ثلاث سنوات وجريمة النصب التى يعاقب مرتكبوها بعقوبة النصب المدرجة في قانون العقوبات.

أما السب والقذف الالكترونى، فتكون جنحة، وإذا كانت الجريمة تركيب صور فاضحة، توجه لمرتكبها، تهم من قبيل، خدش الحياء وهتك العرض والتحريض علي الفسق. أما اطلاق الشائعات والسطو علي أرقام الكروت الائتمانية واقتحام نظم البنوك فتوجه إلي مرتكبها تهم تكدير الأمن العام وتهديد الاقتصاد القومي والاضرار بالمصالح العليا للبلاد وهي اتهامات خطيرة تقود صاحبها الي محاكم الجنايات مباشرة. على أن هذا التكييف القانونى لجرائم المعلوماتية يظل عاجزا عن مواكبة هذه النوعية من الجرائم وما يصاحبها من تطور مستمر فضلا عن تنامى أنواعها وانتشارها بشكل مريب وهو الأمر الذى يحتم على المشرع المصرى سرعة اصدار قانون جديد يواجه الجرائم الالكترونية خاصة ان هناك بعض الجرائم المستحدثة التي لن تجد لها تكييفا قانونيا محددا في القانون التقليدى.

- آليات مكافحة الجريمة الالكترونية فى مصر:

فيما يتعلق بآليات مواجهة الجرائم المعلوماتية، فلا أحد ينكر الجهود الحكومية والأهلية فى مجال المكافحة، فقد أنشأت وزارة الداخلية المصرية

عام 2002، آلية في هذا الاطار تحت مسمى " إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات التابعة للادارة العامة للمعلومات والتوثيق، بالقرار الوزارى رقم 13507 لسنة 2002 [1].

وقد تحددت مهام الإدارة في رصد ومتابعة جرائم التطور التكنولوجي وتتبع مرتكبيها من خلال أحدث النظم الفنية والتقنية الحديثة ويتم تقنين الاجراءات بعد عملية التتبع الفني وضبط القائم بارتكاب الجريمة التي يكون تكييفها القانوني من خلال قانون العقوبات والجريمة التى تتعامل معها الإدارة تتمثل في الأنشطة غير القانونية التي يكون فيها الكمبيوتر وسيلة أو غاية أو كليهما وتتخذ أشكالا متعددة بما فيها الاحتيال باستخدام البطاقات الائتمانية وبيع المواد الالكترونية وانتهاك حقوق الملكية الفكرية في مصر وسرقة البريد الالكتروني والتزوير باستخدام الماسحات الضوئية والطابعات وجرائم الشبكات واختراقها والدخول على أجهزة الحاسب الآلي للغير وسرقة المعلومات التي تمثل سرية خاصة لبعض الأشخاص أو المؤسسات أو الشركات, وقيام البعض بنشر مواقع تسيء لأشخاص آخرين أو تسيء لشكل ومظهر الدولة, ثم ظهرت جرائم عالمية أخرى يقوم بها بعض الهاكرز ومنها إطلاق الفيروسات واختراق المواقع الرسمية أو الشخصية أو اختراق الأجهزة الشخصية وأنظمة شفرات الكمبيوتر للمؤسسات والأفراد، وجرائم التجسس الصناعي، وجرائم الأموال مثل السطو والاحتيال والنصب والجريمة المنظمة، وجرائم المخدرات وغسيل الأموال، وجرائم الآداب وتجارة السلاح وجرائم الابتزاز الإلكتروني، وجرائم الغش الإلكتروني,

(1) راجع : قرار وزير الداخلية المصرى الرقيم 13507 لسنة 2002 بشأن إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات التابعة للادارة العامة للمعلومات والتوثيق، القاهرة 2002.

بالإضافة إلى جرائم القرصنة وجرائم محتوى الإنترنت من المواقع الإباحية أو المعادية سواء دينيا أو سياسيا.

-آلية عمل الإدارة ومراحل التحري والضبط:

تمر القضايا التى ترد إلى إدارة مكافحة جرائم الحاسب الآلى وشبكة المعلومات، بالعديد من الإجراءات، منها: فحص البلاغ في القسم الفني، وتأكيد المعلومات الواردة به، ثم تثبيت الاتهامات عبر القسم الجنائي، ومهمته تحرير المحضر، ثم يعود الملف علي القسم الفني مرة أخري لمتابعة الإيميلات ونصب الكمائن الالكترونية، وتحديد شخصية المتهم، وعنوانه، واعداد تقرير فني برقم التليفون المستخدم في الدخول علي الإنترنت، أو مكان مقهي الانترنت المستخدم في ارتكاب الواقعة، ومن ثم يقوم القسم الجنائي بالتعاون مع قسم العمليات، حيث يتم استصدار إذن من النيابة العامة بضبط جهاز الحاسب الآلي المستخدم في ارتكاب الجريمة، وفحصه، وبعد ذلك يتم تسليم الجهاز إلي القسم الفني ليتولي مثل هذه العمليات، واستخراج الأدلة والصور التي تدين المتهم، ثم يتم إعداد تقرير فني استكمالي لإرفاقه مع المتهم الذي يتم إحالته للنيابة للتحقيق.

فضلا عما تقدم، يتم ضبط الجريمة من خلال بلاغ أو معلومة تصل إلي جهاز الأمن، وتقوم الإدارة بتتبعها وإثباتها بالأدلة وبالأسلوب التقني والفني ومدي الجرم والمخالفة التي تمت وتقديم مرتكبها إلي المحاكمة، ومما يساعد على السرعة فى الإنجاز والأداء أن الإدارة تضم نخبة متميزة من الضباط والفنيين المدربين علي مكافحة جرائم الانترنت، وكيفية التعامل مع أحدث اجهزة الفحص الفني الموجودة بالوزارة للتعامل مع مثل هذه الجرائم والتحفظ عليها بشكل آمن، وسحب كل البيانات، والمعلومات، والصور، بطريقة سليمة لضمها إلي ملف القضية.

- بعض النماذج لجرائم الكترونية فى مصر وآلية التعامل معها:

1- حررت ربه منزل محضرا رسميا في إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالادارة العامة للمعلومات والتوثيق بوزارة الداخلية، أكدت فيه تضررها من قيام زوجها السابق بالتشهير بها عن طريق الانترنت، وقد تبين من الفحص الفني وجود ثلاثة مواقع إباحية بشبكة الانترنت تحتوي علي أفلام مخلة لها وتعليقات علي تلك الأفلام تتضمن عبارات تشهير بها وبزوجها الحالي، كما تبين أن المتهم وهو زوجها السابق ويعمل تاجر أدوات منزلية ارتكب الواقعة انتقاما من الشاكية لوجود بعض القضايا والخلافات بينهما فضلا عن قيامها بالزواج من آخر.

2- لجأت فتاة حاصلة علي بكالوريوس تجارة إلي نفس الإدارة لتحرر محضرا بتضررها من قيام مجهول بإنشاء بروفيل لها علي موقع "الفيس بوك" من خلال شبكة الانترنت، متضمنا بياناتها الشخصية وصورا شخصية خاصة بوالديها وعبارات توحي برغبتها في إقامة علاقات محرمة مع من يرغب، وقد أثبت الفحص الفني أن مرتكب الواقعة وهو خطيب الشاكية السابق قد استخدم جهاز حاسب آليا متصلا بشبكة (ADSL) بها عدد 15 مشتركا. وقد اعترف بارتكابه الواقعة، مبررا ذلك بالانتقام من الشاكية وأسرتها لرفضهم تسليمه الشبكة عقب قيامه بإنهاء الخطبة.

3- مواطنة حاصلة علي بكالوريوس هندسة تتضرر من قيام مجهول بإرسال رسائل بريد إلكتروني علي عنوان البريد الإلكتروني الخاص بها تتضمن عبارات سب وقذف، فضلا عن تهديدها ببعض الصور الشخصية لها.

والجدير بالملاحظة أن إدارة مكافحة جرائم الحاسب بوزارة الداخلية، تستطيع الوصول إلي الشخص الذي يرتكب جريمة الكترونية عن طريق الـ(I.P) وهو العنوان الالكتروني لهذا الشخص فبمجرد دخول أي شخص علي الأنترنت يحصل علي رقم خاص به وعن طريق هذا الرقم يتم تحديد موقعه.

وتشير مصادر بوزارة الداخلية إلى أن جرائم انتهاك حقوق الملكية الفكرية خاصة قرصنة البرمجيات، أدت إلى خسائر كبيرة في منطقة الشرق الأوسط وأفريقيا وهاتين المنطقتين تعدان من المناطق التى شهدت ارتفاعا كبيرا في معدل قرصنة المعلومات بين عامي 2005، 2006، حيث وصلت نسبة انتشار البرمجيات المقلدة إلي 60 % في منطقة الشرق الأوسط.

ومن مظاهر الجهود المبذولة من الإدارة الجديدة تشكيل مجموعات عمل لمتابعة شبكة الإنترنت يوميا على مدى اليوم لمراقبتها وفحص التعاملات والمعاملات التي تتم عليها من وإلى الخارج، وإذا ما ظهر أية مخالفات أو أعمال تمثل خروجا على القانون والشرعية أو تهديد أمن واستقرار الوطن يتم التدخل فورا بالتنسيق مع الأجهزة النوعية الأخرى[1].

ويأتى فى إطار الآليات الخاصة بمواجهة الجرائم الالكترونية فى مصر، آلية الابلاغ عن الجرائم، حيث بإمكان المواطنين الإبلاغ عن الجرائم الإلكترونية عبر الوسائل الآتية:

1- الموقع الإلكتروني لوزارة الداخلية علي شبكة الانترنت (WWW.Moiegypt.gov.eg).
2- اخطار إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بمقر وزارة الداخلية بشارع الشيخ ريحان سواء بالحضور الشخصي أو الاتصال بأرقام تليفونات: 27928484 /27926071 /27924091/27924090.

1 - http://www.ahlalhdeeth.com/vb/showthread.php?t=169760

3- كما يمكن تلقي البلاغات من خلال الخط الساخن (108) والذى تم إنشاؤه مؤخرا لهذا الغرض.

ولا يمكن إنكار الدور الذى تمارسه الجمعية المصرية لمكافحة جرائم الإنترنت فى مجال التصدى لهذا النوع من الجرائم باعتبارها إحدى الآليات الأهلية التى بذلت من جهود فنية وبحثية من أجل الحد من جرائم المعلوماتية والانترنت، **ويمكن رصد بعضا من هذه الجهود فى النقاط التالية:**

1- وقعت الجمعية بروتوكول تعاون مع كلية الحقوق جامعة عين شمس بهدف تثقيف وتدريب طلبة وخريجي كليات الحقوق والآداب والإعلام والسياحة والآثار والتجارة والحاسبات والمتخصصين، والسادة القضاة واعضاء النيابة العامة والسادة المحامين والعاملين في القطاعات القانونية في المؤسسات وتأهيل وإكساب المتدربين المهارات القانونية والعلمية والعملية والفنية الخاصة بارتباط المعلوماتية والاتصالات بتخصصاتهم ومدى تأثير استخدام تكنولوجيا المعلومات في انجاز مهام اعمالهم والتعريف بماهية التعامل مع الاشكاليات القانونية في حقل المعاملات الالكترونية حول موضوعات تشمل كيفية اثبات الشخصية، كيفية التوقيع الالكتروني، أنظمة الدفع النقدي الرقمي (المال الرقمي أو الالكتروني)، سرية وأمن المعلومات من مخاطر إجرام التقنية العالية، خصوصية العميل، المسئولية عن الأخطاء والمخاطر، حجية المراسلات الالكترونية، التعاقدات المصرفية الالكترونية، مسائل الملكية الفكرية لبرمجيات وقواعد معلومات البنك أو المستخدمة من موقع البنك أو المرتبطة بها، علاقات وتعاقدات البنك مع الجهات المزودة للتقنية أو الموردة لخدماتها أو مع المواقع الحليفة، مشاريع الاندماج والمشاركة والتعاون المعلوماتية.

2- مبادرة انطلقت من القاهرة كمبادرة دولية تبنتها الجمعية الدولية لمكافحة الإجرام السيبيرى بفرنسا، بالتعاون مع الجمعية المصرية لمكافحة جرائم الإنترنت، تحمل بارقة أمل لسن قوانين رادعة تحمى رواد شبكة الإنترنت من التجاوزات غير اللائقة التي تحدث على الشبكة، بداية من الإرهاب الإلكتروني ومرورا بالسطو على الحقوق الفكرية، وانتهاء بتجريم تجارة الرقيق الأبيض على الشبكة العنكبوتية وماهية التنظيم القانوني للعالم الإفتراضي بأقسامه من المعاملات القانونية الرقمية وعقود التجارة الإلكترونية وحماية الملكية الفكرية عبر الإنترنت والتعريف بأنماط وأشكال الجرائم عبر الإنترنت وماهية الدليل الرقمي وحجيته في الإثبات وعرض احدث التقنيات الفنية العالمية للتعامل مع مثل هذه النظم.

وغنى عن البيان أن الكثير من أهل الاختصاص فى مجال جرائم المعلوماتية والإنترنت، قد اقرحوا آلية متخصصة تماما فى هذا المجال هى "شرطة الانترنت" كجهة مسئولة عن مكافحة جرائم الإنترنت.

ثالثا: القضاء المصرى والجرائم الإلكترونية: نحو ضرورة إنشاء محكمة إلكترونية

بداية، يجب التأكيد على أن إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للمعلومات والتوثيق بوزارة الداخلية، إنما هى تعمل علي تطبيق القوانين الحالية ومنها قانون العقوبات رقم 58 لسنة 1937 وقانون حماية حقوق الملكية الفكرية رقم 82 لسنة 2002، وقانون تنظيم الاتصالات رقم 10 لسنة 2003، وقانون تنظيم التوقيع الإلكتروني رقم 15 لسنة 2004، والقانون رقم 126 لسنة 2008 بتعديل قانون الطفل رقم 12 لسنة 1996،

فضلا عن قوانين أخري – من المقرر الانتهاء منها- وتشمل قانون الجريمة الإلكترونية وإجراءاتها الجنائية، وقانون التجارة الإلكترونية، وقانون حماية البيانات الشخصية، وتأمين الفضاء الإلكتروني، ويتم اعداد وصياغة تلك القوانين من خلال تعاون وثيق بين أجهزة الدولة التشريعية والتنفيذية والفنية. ومن المؤكد أنه باكتمال صدور تلك التشريعات تكتمل منظومة مكافحة الجرائم الإلكترونية فى مصر.

ومن الجدير بالذكر ان ساحات القضاء المصرى شهدت عشرات القضايا الناجمة عن جرائم الكترونية أغلبها قضايا متعلقة بالتشهير بالأفراد أو النصب والاحتيال، فمثلا شهد عام 2005، صدور أول حكم لجرائم التشهير عبر الإنترنت عندما قضت محكمة جنح مستأنف النزهة بمعاقبة الفلسطيني فيصل عدنان بالحبس لمدة ستة أشهر لإدانته بنشر صور إباحية ومعلومات خاصة عن فتاة خليجية علي شبكة الإنترنت. وقد بدأت القضية ببلاغ من الفتاة لمباحث المصنفات الفنية.

وتأتى ضمن القضايا التى لاقت اهتمام إعلاميا، قضية اقتحام الموقع الإلكتروني لمجلة روز اليوسف التي حدثت في نهاية عام 2005، فقد تقدمت المؤسسة ببلاغ لادارة مكافحة جرائم الحاسبات وشبكة المعلومات عن قيام مجهول باختراق موقع المجلة وتغيير المواد المنشورة، وتمكن ضباط المباحث من خلال التحليل والفحص الفني من تحديد الأرقام التعريفية التي استخدمت في عملية الاختراق وتم ضبط المتهم والجهاز المستخدم بمقر الشركة التي يعمل بها وبفحص الجهاز أمكن التوصل لادلة إثبات أنه هو الشخص الذي اخترق موقع مجلة روز اليوسف[1].

(1)- http://www.ng3awya.com/topic29076.html0

ويؤكد الكثير من رجال القانون على ضرورة إنشاء محكمة إلكترونية لسد الفجوة القانونية التي أحدثها التطور التكنولوجي الهائل في السنوات الأخيرة، فهناك جرائم ترتكب، وحرمات تنتهك، وحقوق تسلب على شبكة الإنترنت دون رقابة قانونية تذكر، والسبب في ذلك عدم وجود قانون دولي رادع يلاحق هواة الإجرام الإلكتروني، ويحاكمهم أمام محاكم دولية، إلا أن ذلك ليس من الأمور البعيدة التي يمكن أن تشق طريقها إلى التطبيق العملي في المستقبل القريب[1].

والمحكمة الالكترونية التى نتحدث عنها، تتطلب - بشكل عاجل- إصدار تشريعات متخصصة فى مجال مكافحة الجريمة الإلكترونية، فضلا عن توفير القضاة المتميزين للقيام على أعمال الفصل فى القضايا المطروحة على هذه المحاكم، على أن يتم تنظيم الدورات اللازمة لتأهيل **القاضى الإلكترونى** وتمكينه من ملاحقة التقدم الكبير فى مجال الجرائم الإلكترونية.

إن الانتشار الكبير للإنترنت في الحياة العملية، أظهر الحاجة في وضع الحلول القانونية للمشاكل الناتجة عن استخدام الإنترنت في ضوء القواعد العامة للقانون إضافة إلى أهمية توجيه نظر المشرع للتدخل لوضع قواعد خاصة لتنظيم استخدام الإنترنت في بعض المجالات الحيوية، كما أن عليه وضع بعض النقاط صوب عينيه في تشريع قانون حماية المعلومات وهي الحماية المدنية لمواقع الإنترنت والإثبات والضوابط الشرعية لاستخدام الإنترنت والتقنية والجريمة المنظمة وتفعيل قانون العقوبات.

وإذا كانت هناك جرائم ذات طابع اقتصادي أو سياسي تلقى اهتماما واسعا من المؤسسات المعنية بمكافحة جرائم الإنترنت، فإن الجرائم الأخلاقية على الإنترنت والتي يقوم بها أكبر مسوقي تجارة الجنس في العالم، كثيرا ما تصطدم

(1) - http://www.moheet.com/show_news.aspx?nid=111727&pg=38

بعوائق تشريعية. ففي مصر مثلا قامت شرطة الآداب بمراقبة 10 آلاف شاذ من المتغربين يعلنون عن عناوينهم على الإنترنت ويبدون استعدادهم لممارسة الفجور، لكن الشرطة لم تستطع إحالتهم إلى المحاكم لأنها لم تستطع إصدار إذن من النيابة لمعاقبتهم؛ لأنهم يمارسون فعلتهم الشنعاء من مواقع خاصة. أما تنظيم الشواذ الذي ألقي عليه القبض بالفعل فقد تجاوزوا الدعوة والتعارف على الإنترنت إلى الالتقاء الفعلي وهو ما مكن الشرطة من إحالتهم إلى القضاء.



المبحث الثانى
تنامى جرائم المعلوماتية والانترنت
فى الدول العربية وآليات مواجهتها

ليست الدول العربية ببعيدة عن مرمى الجرائم الإلكترونية، ذلك أن هذه الجرائم لم تترك بلدا من بلاد العالم إلا واخترقتها ونالت من أهداف محدده فيها، فالسعودية والإمارات وسلطنة عمان والكويت وفلسطين وغيرهم من الدول العربية بادروا إلى وضع - أو فى طريقهم لوضع- تشريعات إلكترونية لمواجهة الجرائم المعلوماتية.

وبالنظر إلي موقع العالم العربي في خريطة استخدام وسائل تقنية المعلومات الحديثة وموقع الدولة بين شقيقاتها الدول العربية فإن إحصائيات الاتحاد الدولي للاتصالات لعام 2001 تشير إلى أن نسبة مواطني العالم العربي، الذين سبق أن استخدموا شبكة الإنترنت، لا يتعدى 1% رغم أن سكان العالم العربي ال 170 مليون نسمة يشكلون5%من مجموع سكان العالم.

وإذا ما قارنا ذلك بنسبة الأوروبيين والأمريكيين التي تفوق 58 في المائة فإن ذلك يدفع البعض إلى وصف تجربة العالم العربي في مجال تكنولوجيا الاتصالات والإنترنت بأنها في مرحلتها "الجنينية".

وإذا لم يكن الحاجز أخلاقيا أو سياسيا فقد يكون تقنيا أو ماليا. إذ تعد معظم شبكات الاتصال في العالم العربي غير متطورة وملكا للقطاع العام. كما تتباين نسبة توفير خدمات الاتصال من بلد عربي لآخر، ففي الوقت الذي نجد فيه أكثر من 100 خط هاتفي لكل 100 منزل في الإمارات والكويت، لا تتعدى النسبة في سوريا ومصر والمغرب حيث الكثافة السكانية كبيرة، خمسين خط هاتفي لكل مائة عائلة.

كما أن نفقات الاتصال لا تزال عالية في بلدان العالم العربي مما يحول دون التشجيع على استخدام الإنترنت بشكل مكثف. فقد تبلغتكلفة ثلاثين ساعة اتصال بالإنترنت شهريا في سوريا 47 دولارا أمريكيا، وفي السعودية 41 دولارا، و 24 دولارا في الإمارات العربية المتحدة، وعشر دولارات في مصر.

ووفقا لدراسة، أعدت لصالح منتدى دافوس الاقتصادي الدولي حول تحديات تطور تكنولوجيا الاتصالات والإعلامفي العالم العربي، تم تصنيف الدول العربية إلى مجموعات ثلاث: مجموعة التطور السريع وتشمل الكويت والإمارات العربية المتحدة، و مجموعة الدول الصاعدة وتشمل كلا من مصروالأردن ولبنان والسعودية، ومجموعة الدول السائرة في طريق النمو وتضم المغرب وعمان وسوريا.

ويمكننا بيان تطور الجرائم الالكترونية فى الدول العربية ووسائل تعاطيها معها من خلال النقاط التالية:

أولا: المملكة العربية السعودية

أعلنت السلطات المختصة أنها ستفرض عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن 500 ألف ريال فيما يعادل 133 ألف دولار لجرائم القرصنة المرتبطة بالانترنت واساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صور دون تصريح، إلا أن المملكة وفى رغبة من أجل تقنين هذا الوضع، أصدرت تشريعا وطنيا فى هذا الخصوص مؤخرا تحت مسمى "نظام مكافحة جرائم المعلوماتية السعودى".

وباصدار هذا التشريع تكون المملكة العربية السعودية[1]، قد سبقت

(1) راجع: "نظام مكافحة جرائم المعلوماتية السعودى" الصادر بالمرسوم رقم م/ 17 بتاريخ 8/ 3/ 1428هـ وطبقا لقرار مجلس الوزراء رقم (79)بتاريخ 7/ 3/ 1428هـ قائمة الملاحق.

نظيراتها من الدول العربية في إصدار قانون جديد لمكافحة جرائم المعلوماتية التي تشمل التهديد والابتزاز والتشهير بالآخرين في مواقع الانترنت وإنشاء مواقع الإنترنت الإرهابية.

وذكرت مصادر بوزارة الداخلية السعودية أن نظام مكافحة جرائم المعلوماتية قد أصبح قيد التطبيق بعد صدور موافقة مجلس الوزراء عليه، باعتباره إطارا قانونيا مهما جدا في تعريف وتحديد الجرائم المعلوماتية والحد منها ومواجهتها بعد أن أصبحت تلك الجرائم من بين الجرائم التي تهدد أمن وسلامة المجتمعات الانسانية.

ويشمل النظام الجديد 16 مادة تتضمن عقوبات صارمة ضد مرتكبي هذه الجرائم تتراوح بين سنة و10 سنوات سجنا وغرامات مالية تصل الى خمسة ملايين ريال سعودي، مضيفا أن النظام تضمن تعريفات المصطلحات والمسميات الواردة في النظام مثل "الشخص" و"النظام المعلوماتي" و"الشبكة المعلوماتية" و"البيانات والجريمة المعلوماتية الى جانب أهداف النظام بالحد من هذه الجرائم والعقوبات المقررة لكل منها.

وحددت مواد النظام الأخرى الجرائم المعلوماتية وعقوباتها التي تنوعت بين السجن لمدد مختلفة والغرامات المالية بحسب نوع وطبيعة كل جريمة من الجرائم المعلوماتية واختصاصات كل من "هيئة الاتصالات وتقنية المعلومات" و"هيئة التحقيق والادعاء العام" في المساندة اللازمة للأجهزة الأمنية لتحقيق أهداف وغايات هذا النظام.

ويهدف النظام الجديد الى حماية المجتمع من جرائم المعلوماتية والحد منها والمساعدة على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية وحماية المصلحة العامة والأخلاق والآداب العامة وحماية الاقتصاد الوطني.

ولقد عانت السعودية فى الفترة الأخيرة من محاولات اختراق مواقع الإنترنت، وكان آخرها، عندما تعرض أحد المواقع التعليمية الحكومية بالسعودية لاختراق استمر عدة ساعات كتب خلالها من قام بالاختراق ورمز لنفسه بالرمز (0) عبارات ينصح من خلالها مشرفي الموقع على الاهتمام بالموقع وحمايته وعدم استخدام برامج تصميم مجانية. وتأخر كثيرا مشرفي موقع إدارة التربية والتعليم بمنطقة تبوك وهو الموقع الذي تم اختراقه، في صيانة الموقع وحل مشكلة الاختراق، حيث ظل فترة طويلة ورسالة الاختراق ظاهرة على واجهته.

الجدير بالذكر أن كثيرا من المواقع الحكومية قد تعرضت مؤخرا للاختراق إما بداعي التطفل أو لوجود كثير من الخلافات بين الجهة الحكومية ومن يقف خلف هذا الاختراق خاصة في المواقع التعليمة الحكومية مما اضطر مسؤولي وزارة التربية والتعليم السعودية و مؤخرا لنفي اختراق موقعه الخاص بشؤون المعلمين

وبدأت السعودية فى التفكير فى تطبيق قانون الحبس في جرائم الإنترنت عندما أعلنت السلطات هناك أنها سفرض عقوبات بالحبس لمدة عام واحد وغرامات لا تزيد عن 500 ألف ريال لجرائم القرصنة المرتبطة بالانترنت وإساءة استخدام كاميرات الهواتف المحمولة مثل التقاط صور دون تصريح.

الجدير بالذكر أن هيئة الأمر بالمعروف والنهي عن المنكر في السعودية، قد عارضت الهواتف ذات الكاميرات، وحظرت السعودية بيع هذه الأجهزة لعدة أشهر عام 2004، غير أن تلك القيود فشلت في وقف انتشار أحدث الصيحات التكنولوجية في البلد الذي يقطنه 24 مليون نسمة غالبيتهم من صغار السن ويتمتعون بمعدلات دخول فردية مرتفعة.

وتفرض السعودية رقابة شديدة على استخدام الانترنت من خلال تعقب المستخدمين وحظر المواقع الجنسية وبعض المواقع ذات المحتوى السياسين

فبعد ازدياد الخطر من استخدام الانترنت بدأت العديد من المنظمات والهيئات إلى إطلاق الدعوات والتحذيرات من خطورة هذه الظاهرة التى تهدد كل مستخدمى الإنترنت خاصة بعد تقرير برلمانى وضعته لجنة العلوم والتكنولوجيا في مجلس اللوردات البريطانى أظهر أن شبكة الانترنت تحولت إلى حلبة يرتع فيها المجرمون، وتنفذ فيها العصابات عمليات سرقة الأموال من الحسابات المصرفية، محذرا الحكومات والمؤسسات والشركات المختصة التدخل لتنظيم عملها قبل فوات الأوان.

ومن المفيد فى هذا الصدد، التاأكيد على أن اقتصاد الظل الخفي يزداد انتعاشا بفضل الجرائم الإلكترونية التي تدفع إلى الإحساس بأن الانترنت تحول إلى منطقة شبيهة بـ" الغرب المتوحش" في أمريكا في عهودها الأولى، حيث تنعدم سيادة القانون.

ومن المخاطر الكبيرة أن المصارف حول العالم فقدت ملايين الجنيهات الاسترلينية، بسبب الاحتيال المصرفي، منها مبالغ خسرتها المصارف البريطانية عام 2010 والتى وصلت إلى أكثر من 67 مليون دولار.

وفى هذا الصدد، اقترح الباحثون إنشاء شرطة معنية بالمعلومات والإنترنت في السعودية، تحت مسمى "شرطة الإنترنت"، تكون مهامها تطهير الإنترنت وحجب المواقع الإرهابية والمواقع الضارة على المجتمع، لافتة إلى أهمية إنشاء مجلس وطني للمعلوماتية والإنترنت لاقتراح القواعد والتشريعات الخاصة.

ولقد حققت تجربة شرطة الانترنت نجاحا كبيرا في دول كثيرة مثل الصين وأمريكا ومؤخرا دولة فيتنام، مما يعزز مقترحا آخر يمثل إنشاء مجلس وطني للمعلوماتية والإنترنت له سلطة تقنية وأمنية يكون من ضمن مسؤولياته اقتراح القواعد والتشريعات الخاصة بالمعلوماتية والإنترنت.

ومما يعزز ضرورات إنشاء هذا المجلس أن سيكون من بين مسئولياته،

إعداد تقارير إحصائية ومتابعة ما تم عالميا، واستقبال الشكاوى من الأفراد والمؤسسات وإرسال الشكاوى إلى إدارة الاتصال بالشرطة الدولية ووضع معايير للسياسات الوطنية، وتحديد المسؤولية بين الجهات ووضع تعريفات محددة لكافة المصطلحات بالإرهاب وتقنية المعلومات.

هذا ويتضمن النظام السعودي في قوانينه جريمة إنشاء موقع إرهابي على الإنترنت وفقا للمادة السابعة من نظام مكافحة جرائم المعلوماتية على أنه «يعاقب بالسجن مدة لا تزيد على 10 سنوات وبغرامة لا تزيد على 5 ملايين ريال، أو بإحدى العقوبتين، كل شخص يرتكب أيا من الجرائم المعلوماتية التي تتضمن إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، والدخول غير المشروع إلى الموقع الإلكتروني أو النظام المعلوماتي».

ومما يستلزم التأكيد عليه، ضرورة التدخل لمواجهة القصور في التشريعات والقوانين الحالية أو تحديثها بالنص صراحة على تجريم استخدام التقنيات العلمية الحديثة بالإضرار بأمن الدولة من الداخل والخارج، والسعي إلى وضع قانون للإنترنت يشتمل في أحد جوانبه على جرائم الإنترنت بشقيها الموضوعي والإجرائي، فضلا عن ضرورة إنشاء منظمة عربية لتنسيق أعمال مكافحة الإرهاب عبر الإنترنت وتشجيع قيام اتحادات عربية تسعى للتصدي لمثل تلك الجرائم، وكذلك تفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة تلك الجرائم عبر نظام الأمن الوقائي.

وفى سبيل تفعيل آليات العمل والتعاون الدولى فى مجال مكافحة الجرائم الإلكترونية، فإنه من الأهمية بمكان التنسيق وتبادل المعلومات والخبرات مع الأجهزة المعنية بمكافحة الإرهاب عبر الإنترنت في كافة دول العالم، ونقل التقنية التي تستخدم في الدول المتقدمة في مكافحة الإرهاب الإلكتروني، والتوسع في دراسة فكر التنظيمات الإرهابية التي تبث عبر شركة الإنترنت، وتعزيز التعاون مع المؤسسات الدولية المعنية خاصة "الإنتربول" لمواجهة

كافة أشكال الجرائم، إضافة إلى الإسراع في الانضمام إلى المعاهدات الدولية الخاصة بمكافحة جرائم الإنترنت[1].

ثانيا: مملكة البحرين

لا توجد قوانين خاصة بجرائم الإنترنت، وإن وجد نص قريب من الفعل المرتكب فإن العقوبة المنصوص عليها لا تتلائم وحجم الأضرار المترتبة على جريمة الإنترنت.

ثالثا: سلطنة عمان

أصدرت السلطنة المرسوم السلطاني رقم 2001/72 الذي تضمن جرائم الحاسب الآلي وحدد فيه الجرائم التالية:

- الالتقاط غير المشروع للمعلومات أو البيانات.
- الدخول غير المشروع على أنظمة الحاسب الآلي.
- التجسس والتصنت على البيانات والمعلومات.
- انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم وتزوير البيانات أو وثائق مبرمجة أيا كان شكلها.
- إتلاف ومحو البيانات والمعلومات.
- جمع المعلومات والبيانات وإعادة استخدامها.
- تسريب البيانات والمعلومات.
- نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكا لقوانين حقوق الملكية والأسرار التجارية..

رابعا: فلسطين

لا يوجد تشريع خاص يتعلق بجرائم الكمبيوتر والإنترنت إلا أنه يمكن ملاحقة هذه الجرائم عن طريق تطويع نصوص قانون العقوبات الفلسطيني

(1) جريدة الشرق الاوسط 4 يوليو 2010.

بحيث ينطوي تحت لوائها بعض الجرائم المتعلقة بالكمبيوتر كنصوص جرائم السرقة والنصب وخيانة الأمانة والإتلاف وغيرها. ولكن يهمنا أن نشير إلى أهمية التطور التشريعي لتحديد ماهية السياسة الجنائية الواجب إتباعها وفقا للقانون الأساسي المعدل 2003م، والذي أشتمل على الضمانات الدستورية الخاصة بمكافحة الجريمة ومن بينها إذ انه لا جريمة ولا عقوبة إلا بنص قانوني، ولا توقع عقوبة إلا بحكم قضائي، ولذلك فقد استطاعت السلطة الوطنية في فترة وجيزة من الزمن من إصدار حزمة من التشريعات القضائية المتطورة منها قانون السلطة القضائية، وفانون الإجراءات الجزائية، وقانون الإجراءات المدنية والتجارية، وما زال هناك مجموعة من التشريعات الجنائية المهمة تحت الإجراء في المجلس التشريعي من بينها مشروع قانون العقوبات والذي تعرض وبشكل مباشر في المواد(393-397) من الفصل السادس منه لجرائم الحاسب الآلي وهناك مشروع قانون الإنترنت والمعلوماتية، والذي مازال تحت الإعداد في ديوان الفتوى والتشريع بوزارة العدل والذي تضمن العديد من القواعد والأحكام والجرائم والعقوبات المستحدثة فيما يتعلق بالإنترنت والمعلوماتية.

ويلاحظ أن قانون العقوبات الفلسطيني لسنة 1936به من النصوص ما تكفي لمعالجة جرائم الجنس عبر الإنترنت وإخضاعها للعقاب الجنائي خاصة في الفصل السابع عشر منه المتعلق بالجرائم التي تقع على الآداب العامة، وذلك وفقا لأحكام المواد من 151الى 169 من القانون، كما أولى المشرع الجنائي الفلسطيني عناية وأهمية لهذه الجرائم في مشروع قانون العقوبات، والذي خصص له الفصل الثامن بعنوان (البغاء وإفساد الأخلاق)[1].

(1) راجع : قانون العقوبات الفلسطينى الصادر 1936.

وبالرجوع إلى قانون العقوبات الفلسطيني لسنة 1936 فانه يمكن تعريف القدح وفقا للمادة 201 منه على النحو التالي (كل من نشر بواسطة الطبع أو الكتابة أو الرسم أو التصوير أو بأية واسطة أخرى غير مجر د الإيماء أو اللفظ أو الصوت وبوجه غير مشروع مادة تكون قذفا بحق شخص ، بقصد القذف بحق ذلك الشخص، يعتبر انه ارتكب جنحة وتعرف تلك الجنحة بالقدح).

كما يعرف القانون الذم في المادة 202 منه على النحو التالي(كل من نشر شفويا وبوجه غير مشروع أمرا يكون قذفا بحق شخص آخر قاصدا بذلك القذف في حق ذلك الشخص، يعتبر انه ارتكب جنحة ويعاقب بالحبس مدة سنة واحدة وتعرف هذه الجنحة بالذم.

وتعرف المادة 203 من القانون القذف على النحو التالي (تعتبر المادة مكونة قذفا إذا اسند فيها إلى شخص ارتكاب جريمة أو سوء تصرف في وظيفة عامة أو أي أمر من شأنه أن يسئ إلى سمعته في مهنته أو صناعته أو وظيفته أو يعرضه إلى بغض الناس أو احتقارهم أو سخريتهم).

إضافة إلى المواد المذكورة أعلاه فان مشروع قانون العقوبات قد تضمن بين أحكامه هذه الجرائم حيث خصص لها الفصل الرابع عشر منه بعنوان (الاعتداء على الشرف والاعتبار) وفقا لأحكام المواد 323،324، 325،326،327،328،329،330،331.،

ومن جماع هذه النصوص العقابية يمكن توقيع عقوبة القذف والسب العلني أو غير العلني أو القذف بطريق الهاتف على من يقوم بإرسال شتائم إلى الغير بواسطة شبكة الإنترنت وسواء تم ذلك عن طريق إنشاء موقع خاص على شبكة الإنترنت لسب أو قذف شخص معين ، أو سواء كان السب أو القذف عن طريق إرسال بريد إلكتروني للشخص المجني عليه.

وبالنسبة للتشريع الفلسطيني نجد أن القانون الأساسي المعدل لسنة 2003 وقانون العقوبات يحميان الحياة الشخصية للمواطن من أي اعتداء عليها.

فالمادة 32 من القانون الأساسي المعدل تنص على (كل اعتداء على أي من الحريات الشخصية أو حرمة الحياة الخاصة للإنسان وغيرها من الحقوق والحريات العامة التي يكفلها القانون الأساسي أو القانون ،جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم ، وتضمن السلطة الوطنية تعويضا عادلا لمن وقع عليه الضرر.هذا وقد عالج قانون العقوبات لسنة 1936 هذه الجرائم في الفصل الثامن والعشرون منه والذي جاء بعنوان الجرائم التي تقع على الحرية الشخصية .إضافة إلى ذلك فان مشروع قانون العقوبات الذي مازال تحت الإجراء خصص الفصل الحادي عشر منه إلى جرائم الاعتداء على الحرية الشخصية والحياة الخاصة، وذلك وفقا لأحكام المواد (300، 301، 302، 303، 304، 305، 306، 307، 308، 309، 310، 311، 312، 313، 314).

ونشير هنا إلى المادة 309 منه التي تنص على ((يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة لأحد الأشخاص ، بان ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانون أو بغير رضاء المجني عليه:

أولا : استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه حديثا خاصا جرى في أحد الأماكن أو عن طريق الهاتف.

ثانيا : التقط أو نقل أو نسخ أو أرسل بأي جهاز من الأجهزة صورة شخص في مكان خاص، وإذا صدرت الأفعال المشار إليها أثناء اجتماع على مسمع ومرأى الأشخاص الذين يهمهم الأمر الحاضرين في ذلك الاجتماع فان رضاء هؤلاء يكون مفترضا ما لم يبدوا اعتراضهم على الفعل.

ثالثا : أساء عمدا استعمال أجهزة الخطوط الهاتفية ، بأن أزعج الغير أو وجه إليهم ألفاظا بذيئة أو مخلة بالحياء أو تضمن حديثه معهم تحريضا على الفسق والفجور.

خامسا: الإمارات العربية المتحدة

شهدت دولة الأمارات في السنوات الأخيرة ثورة اقتصاديه وتقنيه هائلة، وتطورت فيها الأعمال بشكل ملحوظ ،وأصبحت بحسب تصنيف الكثير من الجهات العالمية والعربية من أكثر الدول العربية في مجال استخدام ،الحاسب الآلي وشبكة الإنترنت.

وقد قطعت دولة الإمارات العربية المتحدة شوطا كبيرا فى مجال تكنولوجيا المعلومات من خلال إقامتها لمدينة الإنترنت، وسعيها إلى رفع نسبة استخدام الشبكة الإليكترونية بين سكانها إلى 38% مع مطلع عام 2005، في وقت لا تتعدى فيه نسبة الحاسبات الشخصية في سوريا 1.6 % بالنسبة لكل 100 ساكن أو 36 مستعملا للإنترنت من بين كل عشرة آلاف مواطن، بالنظر إلى كل هذا يتضح عمق الهوة الرقمية التي على العالم العربي.

هذا وتتصدر الإمارات العربية المتحدة الدول العربية من حيث نسبة مستخدمي الإنترنت من بين سكانها حيث بلغت لديها 29،9% ، لتتبعها البحرين بنسبة 18،17% ، ثم قطر بنسبة 12،81 %، فالكويت بنسبة 11،29%. على حين يقف في أخر القائمة العراق بنسبة 0،08%،وقبله.السودان بـ 10،10%

وإذا كان هذا هو موقع دولة الأمارات في خارطة استخدام الحاسب الألي وتقنيات الاتصال الحديثة، فإنه من الطبيعي أن تكون الدولة مطمعا لذوي النفوس الضعيفة من طالبي الثراء السريع، الذين يبحثون عن المال من مصادره غير المشروعة، أو من أولئك الأشخاص الذين سخرو طاقاتهم الذهنيه لا لأكتشاف النافع المفيد، وانما لأشباع غرور الذات لديهم وذلك من خلال محاولة الوصول الي أنظمة المعلومات، في الشركات والبنوك والمؤسسات، أو المنازل بدون وجه حق، بقصد الأفساد والتخريب، أو لمجرد العبث والمتعه، وهم المسمون باسم(الهاكرز).

ناهيك عن أولئك الذين وجدو في الحاسب الألي وشبكة المعلومات بيئة خصبة لأرواء نزواتهم المنحرفه، والسعي لهدم قيم وأخلاق المجتمعات من خلال انتاج وترويج البرامج الضارة بالفكر السليم والأخلاق والأداب السامية للمجتمع العربي المسلم.

تشريعات مكافحة جرائم تقنية المعلومات في دولة الأمارات:

يعتبر قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (2) لسنة 2006[1]، من أحدث التشريعات العربية في هذا المجال، والذي تم اقتراحه من قبل الدولة وإعتماده لدى الأمانة العامة لمجلس التعاون لدول الخليج العربية كمسودة لمشروع قانون خليجي موحد لمكافحة جرائم تقنية المعلومات، وتم إعتماد صيغة المشروع في الإجتماع العاشر لوكلاء وزارات العدل بدول مجلس التعاون المنعقد بمدينة أبوظبي في شهر سبتمبر 2006.

على أنه من الضرورى أن نتعرف على القوانين الإماراتية فى مجال الاتصالات وتكنولوجيا المعلومات والتى كانت بمثابة آليات الدولة الوطنية فى ملاحقة المجرم الالكترونى، وفيما يلى بيان بهذه القوانين:

نصوص قانون العقوبات الإتحادي رقم 3 لسنة 1987:

لقد وردت في قانون العقوبات بحكم أنه القانون الجنائي العام تقسيمات كثيره للجرائم[2]، منها مايقع على أمن الدولة الداخلي والخارجي، والجرائم الواقعة على الأموال (مثل جريمة السرقه، والنصب، وخيانة الأمانه والأتلاف)، والجرائم الواقعة على الأشخاص كالجرائم المتعلقه بحرمة الحياة الخاصة، والجرائم المتعلقة بالسمعة، والجرائم الماسة بالآداب العامة،

---

(1) راجع القانون الاتحادى رقم 2 لسنة 2006 بشأن مكافحة جرائم المعلومات، أبو ظبى 2006.

(2) راجع قانون العقوبات الاتحادى رقم 3 لسنة 1987، أأبو ظبى 1987.

وجريمة التهديد) ،والجرائم الماسة بالعقيدة والأديان، والجرائم الخاصه بوسائل المواصلات والإتصالات، وغيرها من الجرائم، وعلى ذلك فإن قانون القوبات الإتحادي وإن كان لاتوجد به نصوص خاصة، لجرائم الحاسب الألي، أو جرائم الشبكات إلا أن العديد من الجرائم الواردة فيه، يمكن أن يستخدم الحاسب الآلي في ارتكابها كوسيلة أو أداة متتمة للجريمة، وبالتالي إذا تم في مرحلة التحقيق إدانة المتهم، والوصول الي مرحلة اسناد التهمة اليه وفق نصوص قانون الأجراءات الجزائيه، وتحققت في حقه أركان الجريمه الموصوفه في قانون العقوبات الإتحادي فإنه سينال العقوبه الواردة في هذا القانون وخاصة أن هناك مبدأ قانوني مقرر بالمادة (42) من قانون العقوبات نصها(لايعتبر الجهل بأحكام هذا القانون عذرا) هذه قاعده مسلم بها في جميع التشريعات الجنائيه، وبالتالي لايمكن لشخص ان يتعلل بأنه لا يعلم أن ارتكاب الجرائم عن طريق الحاسب الألي ليس مجرما أو ليس له نصوص خاصة، مادام فعله يشكل جريمه تنطبق عليها أوصاف وأركان الجريمه الوارده بقانون العقوبات الإتحادي، وذلك تحقيقا لمبدأ المشروعية، أو الشرعية الجنائية، ومقتضاه انه لاجريمه ولا عقوبه إلا بنص ، فحيثما وجد هذا النص سواء في قانون خاص او عام، وارتكب شخص ما الفعل المحظور بموجب ذلك النص فإن الجريمه تقع ،ويصبح من المشروع معاقبة مرتكبها، بغض النظر عن مسمى القانون، أو مكان ورود النص المحرم للفعل

ومن أمثلة الجرائم التي يمكن ان ترتكب عن طريق أجهزة الحاسب الألي والأجهزه المرتبطه بها ويمكن معاقبة مرتكبيها بالعقوبات الوارده بقانون العقوبات الأتحادي ،الجرائم الأتيه:

1- جريمة تخريب أو تعطيل وسائل الاتصال الدولية:

حيث نصت المادة (21) على انه ((يسري هذا القانون على كل من وجد في الدولة بعد ان ارتكب في الخارج بوصفه فاعلا او شريكا في جريمة

تخريب او تعطيل وسائل الاتصال الدوليه أو جرائم الاتجار بالمخدرات أو في النساء أو الصغار أو الرقيق أو جرائم القرصنة ،والإرهاب الدولي)).

ولاشك ان مدلول عبارة - وسائل الاتصال الدولية - يشمل شبكة الإنترنت العالمية، وبذلك يكون القانون قد أخذ بمبدأ التضامن الدولي لمكافحة الجرائم العابرة للحدود، والجرائم المنظمة، وهذا النص يعتبر من النصوص الفريدة في قانون العقوبات، الذي صدر في عام 1987، وعليه فإنه بموجب هذا النص يمكن معاقبة من يعطل عمل شبكة (الإنترنت) بأية وسيله - كزرع الفيروسات مثلا-، ولو لم يكن فعله قد تم في الدوله، فإنه يمكن ملاحقته إذا وجد في الدولة بموجب هذا النص، وتقديمه للمحاكمة ليأخذ جزاءه العادل بشرط ألا يكون قد تمت محاكمته في مكان آخر عن هذه الجريمه.

2- جريمة التهديد:

من المتصور أن تتم جريمة التهديد المنصوص عليها في القانون عن طريق الحاسب الآلي، وذلك عن طريق، كتابة التهديد في برنامج معين أو نشره على صفحة الويب، أو إرسال رسالة تهديد برسالة إلكترونيه (إميل)، أو اثناء المحادثة التي تتم في غرف الدردشه (الشات) أو المنتديات ،أو غرف المحادثه (البالتوك)، كما نصت المادة (351) من قانون العقوبات على أنه (يعاقب بالسجن مدة لا تزيد على سبع سنوات من هدد آخر بأرتكاب جناية ضد نفسه أو ماله أو ضد أومال غيره أو بإسناد امور خادشه بالشرف أو إفشائها، وكان ذلك مصحوبا بطلب أو بتكليف بأمر أو الامتناع عن فعل أو مقصود به ذلك)).

على أنه ورد النص على التهديد البسيط في المادة (352) وهو التهديد الذي لا يصحبه طلب أو تكليف بأمر أو امتناع ،وعاقب على هذا النوع بالحبس .

والملاحظ في هذين النصين أن القانون لم يورد النص على وسيلة التهديد هل هي الكتابه، أو المشافهة، على عكس ماورد في نص قانون

العقوبات المصري مثلا. وعليه فإن التهديد يقع بأية وسيله يتم بها وصوله الي علم المجني عليه، ومنها الوسائل التقنية الحديثة، وقد صدرت في بعض الدول أحكاما بتطبيق قانون العقوبات على جريمة التهديد عن طريق الانترنت.

3- جريمة تعطيل أو إتلاف وسائل الإتصالات السلكيه واللاسلكيه:

نظرا لأهمية وسائل الاتصالات السلكية واللاسلكية الحديثة في الحياة ولأنها أصبحت شريانا رئيسيا في جسم المجتمع النابض بالحركة والنشاط، والتطور وأصبحت هذه الوسائل عليها مدار التواصل الشخصي، والاقتصادي، والأمني، والعلمي، والتجاري، وعليها تتوقف حياة أشخاص وموتهم، وبتعطلها قد تتكبد الشركات، والدول، والأفراد خسائر جمة تصل إلي المليارات، فإن المشرع أولاها الاهتمام اللائق، وجرم كل إعتداء عليها يؤدي إلي تعطيلها، أو الإضرار بها.

ولا شك أنه يدخل في عمومية هذا النص، الاتصال والتواصل عبر شبكات الانترنت الداخليه، أو العالمية، فهي وسيلة اتصالات لاسلكية، أضحت أكثر أهمية وأكبر أثرا في الحياة من الهاتف أو الفاكس والبرق، فإذا انصبت الجريمة على تعطيل الشبكة المخصصة لمنفعة عامة فإن نص المادة التالية يمكن تطبيقه على هذه الجريمة بحيث ينال الجاني جزاءه العادل.

وفي هذا الصدد ورد النص في المادة (279) عقوبات على أنه (يعاقب بالسجن مدة لا تزيد على عشر سنوات كل من عطل عمدا وسيلة من وسائل الاتصال السلكية، واللاسلكية المخصصة لمنفعة عامة أو قطع أو أتلف شيئا من أسلاكها أو أجهزتها أو حال عمدا دون إصلاحها، وتكون العقوبه السجن مدة لاتقل عن خمس سنوات إذا ارتكب الجريمه في وقت حرب أو فتنة أو هياج أو باستعمال مواد مفرقعة أو متفجرة).

4- الجرائم الماسة بالآداب العامة

إهتم المشرع الإماراتي بحماية الآداب العامة في المجتمع حفاظا على المبادئ والقيم الإسلامية والعربية الأصيلة من العبث، وحفاظا على طهارة المجتمع وسمو أخلاقه، وحفاظا على أبنائه من العادات الدخيلة التي تصرف العقول والطاقات عن الإبداع والعطاء المفيد الي الخنوع والجري وراء السراب الملهي، والملذات الفانية، وإذا كانت جرائم الإخلال بالآداب العامة لها صور كثيرة وحسب المشرع أنه عالج ما شاع منها وظهر واستشرى واشتهر، ووصل إلي حد المساس بقيم المجتمع، والنظام العام فيه. وعلى ذلك كان لظهور وسائل تقنية المعلومات الحديثه، وشيوع شبكة الانترنت، وكسرها لحواجز الحدود بين الدول، وتسلقها لجدران الستر بين البيوت والمساكن، أثر كبير في شيوع جرائم الإخلال بالآداب العامة، لأن أصحاب النفوس الضعيفة، وعصابات الترويج للجنس المبتذل، والفجور وإفساد الأخلاق، وجدت في هذه الأجهزة الحديثة، وشبكات الإنترنت، بيئة خصبة للترويج لأنشطتها وترويج بضائعها الفاسدة القبيحة، حتى أضحت المواقع، والصفحات التي تبث مواد مقروءة، أو صورا، ومقاطع أفلام، أو رسومات تتعلق بالجنس والممارسات الشاذة، تعد بعشرات الملايين، ناهيك عن تجارة الرقيق الأبيض، وجرائم استغلال الأطفال والنساء في الأمور المخلة بالآداب.

وليس بخاف أن دولة الإمارات - في السنوات الأخيرة- قد شهدت بعض نماذج لجرائم مخلة بالآداب العامة، مثل تصوير فتيات وبث صورهن على شبكة الأنترنت، أو سرقة صور مخزنة في حاسبات شخصية وإعادة بثها بعد التلاعب بها ووضعها في مواقع تبث صورا إباحية، ناهيك عن استخدام، الهواتف المتحركة المزودة بكاميرات، لتصوير الأشخاص بدون رضاهم وبثها على الملأ أو تصوير مشاهد مخلة بالآداب أو ممارسات شاذة وبث تلك الصور عبر الشبكة العالمية أو عن طريق خاصية التراسل بين الهواتف بتقنية (البلوتوث) أو غيرها من الطرق وبشكل عشوائي.

ومن جرائم الإخلال بالآداب والتحريض على الفجور والتي وردت في مواد القانون الإماراتي مايلي:

أ- الجهر بما يخالف الآداب، أو إغراء الغير علانية بالفجور:

ورد النص على هذه الجرائم في المادة(361)، حيث نصت على(يعاقب بالحبس مدة لاتزيد على ستة شهور وبغرامة لا تزيد على خمسة آلاف درهم أو بأحدى هاتين العقوبتين كل من جهر بنداء أو أغان أو صدر عنه صياح لأي خطاب مخالف للآداب وكل من جهر علانية بالفجور بأية وسيلة كانت)

ولعل المعول عليه في هذا النص بصدد الجرائم محل البحث هو الجهر علانية بما فيه مخالف للآداب العامة، والأمر الثاني هو إغراء الغير بالفجور بأية وسيلة كانت، والعلانية حسب ما وضحها شراح القانون.

على أن العلنية تتحقق هنا بصدور النداء أو الصياح أو الغناء أو الخطاب المخالف للآداب في مكان عام أو خاص طالما أن هناك أشخاص يسمعون ما يجهر به الفاعل لأن الغرض هو حماية الجمهور من كل ما يخدش كرامتهم وإحساسهم .

وفي مجال الإغراء الذي هو إغواء المجني عليهم وتحبيذ الفجور وتسهيل أمره لهم اشترط القانون العلنية ولم يقيد الوسيلة، وباستخدام شبكة الإنترنت لإتيان هذه الأفعال المجرمة قانونا من قبل الجاني، فإن تطبيق نص هذه المادة على الجريمة والجاني يصبح أمرا يسيرا ويحقق حماية في كثير من الحالات.

ب- تجريم نشر وتوزيع وعرض الصور والأفلام والرسومات المخلة بالآداب العامة:

أما المادة رقم (362) فقد جرمت وعاقبت بذات العقوبة الواردة بالمادة (361)المشار اليها سلفا، حيث نصت على (كل من صنع أو استورد أو صدر أو حاز أو أحرز أو نقل بقصد الاستغلال أو التوزيع أو العرض على

الغير كتابات أو رسومات أو صورا، أو أفلاما أو رموزا أو غير ذلك من الأشياء إذا كانت مخلة بالآداب العامة. ويعاقب بالعقوبة ذاتها كل من أعلن عن شيء من الأشياء المذكورة)، فهي إذن خمسة أفعال مختلفة، جرمتها المادة ولكن بشرط خاص ألا وهو اتجاه قصد الجاني إلي استغلالها أو توزيعها أو عرضها على الغير.

قانون مؤسسة الإمارات للاتصالات رقم 1 لسنة 1991:

ينظر إلى هذا القانون باعتباره القانون الأول المنظم لشئون الاتصالات السلكية واللاسلكية بالإمارات، قبل صدور قانون تنظيم قطاع الاتصالات رقم (3) لسنة 2003[1]، وقد أنشأ هذا القانون مؤسسة الإمارات للاتصالات وحدد أهداف المؤسسة وأغراضها واختصاصاتها وأعطى القانون المؤسسة دون غيرها حق نقل الاتصالات السلكية واللاسلكية وتشغيل وصيانة وتطوير نظام الاتصالات العامة بأسرة في الدولة، وكذلك بين الدولة والخارج وفقا لأحكامه، ونظم هذا القانون حيازة واستعمال أجهزة الاتصالات وتراخيص الحيازة والاستعمال، وحدد شروط ومقابل الخدمات التي تقدمها المؤسسة وذلك بموجب عقود تبرمها مع المنتفعين، وغيرها من الأحكام اللازمة، واشتمل القانون في الفصل السادس عشر منه على العقوبات التي توقع على مخالفة أحكامه، حيث وردت به عدة مواد تتضمن تجريما لبعض الأفعال والعقوبات المقررة للجريمة، فالمادة الأولى مثلا هى مادة عقابية عامة برقم (45) نصها الأتي: (مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون آخر يعاقب كل من يخالف أحكام هذا القانون بغرامة لاتزيد على عشرة آلاف درهم (10000).

(1) أنظر: قانون مؤسسة الإمارات للاتصالات رقم 1 لسنة 1991 وكذا قانون تنظيم قطاع الاتصالات رقم (3) لسنة 2003.

والمادة الثانية برقم (46) نصها الأتي (يعاقب بالحبس لمدة لاتزيد عن ستة أشهر أو بالغرامة التي لاتزيد عن عشرة آلاف درهم:-

أ- كل من يختلس أو يسرق أو يحول أو يقوم بغير وجه حق باستغلال أو استعمال أي خدمة هاتفية أو أي تيار أو خلافة مما قد يستعمل لتوصيل أو نقل الخدمات الهاتفيه أو غيرها من خدمات الاتصالات.

ب- كل من يستغل الأجهزة أو الخدمات أو التسهيلات التي تقدمها المؤسسة في الأساءة أو الأزعاج أو إيذاء مشاعر الأخرين أو أي غرض آخر غير مشروع.

ويجوز للمؤسسة ودون إذن مسبق أن تضع تحت المراقبة أي جهاز أو خلافة إذا توفرت لديها أسباب معقولة للإعتقاد بأنه يستغل في أي مخالفة من المخالفات المنصوص عليها في البند (أ) من هذه المادة أو بناء على طلب المتضررين المشار اليهم في البند (ب) من هذه المادة.

وفي جميع الأحوال لا يجوز للمؤسسة التنصت على محتوى أو مضمون المكالمات دون إذن مسبق من السلطات القضائية المختصة).

وقد أجمع رجال القانون والقضاء فى الإمارات على أن هذا القانون الخاص بمؤسسة الامارات للاتصالات - وبما حواه من نصوص تجريمية- هو القانون المعول عليه في ملاحقة الجرائم التي ارتكبت عبر شبكة الإنترنت للوصول إلي أجهزة الحاسوب الشخصية أو التابعة للمؤسسات أو البنوك والشركات خلال الأعوام المنصرمة، وذلك لأن خدمة الأنترنت تعتبر من الخدمات التي تقدمها مؤسسة الإمارات للاتصالات بموجب عقد بينها وبين المنتفعين، وعليه فإن أي اساءة أو استخدام غير مشروع لتلك الخدمة بالمخالفة لأحكام هذا القانون كانت تعطي للجهات الأمنية وجهات التحقيق القضائية (النيابة العامة) المكنة من تقديم المخالفين ومرتكبي الجرائم التقنية الحديثة إلي العدالة، استنادا لهذه المواد وكذلك مواد قانون العقوبات الإتحادي

على ما سنراه من خلال استعراضنا للجرائم التي تم ضبطها ، في السنوات الأخيرة وتم تقديم مرتكبيها للعدالة، قبل صدور قانون مكافحة جرائم تقنية المعلومات في شهر يناير2006.

ولعل مما سهل على جهات التحقيق تقديم مرتكبي جرائم تقنية المعلومات للعدالة استنادا لنصوص هذا القانون الطريقة التي صيغت بها نصوص هذه المواد فهي نصوص مرنة وبها مترادفات عدة، وفيها من العمومية ما جعل الاستناد إليها يسيرا في أغلب الأحيان وخاصة إذا كانت الجريمة مرتكبة عن طريق استغلال شبكة الإنترنت التي تعتبر خدمة من خدمات الاتصالات، أو عن طريق استخدام أجهزة الأتصال الأخرى، ففي البند (أ) من المادة (46) المشار إليها وردت عبارة (أو غيرها من خدمات الاتصالات) بعد أن ذكر الخدمة الهاتفية أو أي تيار أو خلافه مما قد يستعمل لتوصيل أو نقل الخدمات الهاتفية، كما ورد في البند (ب) الفاظ عامة ومترادفات شاملة تسهل على المحققين الاستعانة بالنص لتقديم كل من يرمي إلي غرض غير مشروع أو إلي إيذاء الآخرين عن طريق استخدام خدمات مؤسسة الاتصالات؛ حيث جاء النص بلفظ(كل من يستغل الأجهزة أو الخدمات أو التسهيلات التي تقدمها المؤسسة في الإزعاج أو إيذاء مشاعر الآخرين أو أي غرض آخرغير مشروع) ليأتي بعد ذلك دور محكمة الموضوع لتكييف طبيعة العمل غير المشروع، وطبيعة الإساءة التي ارتكبها الشخص الجاني، والمادة العقابية المنطبقة سواء من هذا القانون أو قانون العقوبات الإتحادي.

على أنه في كثير من الجرائم المرتبطة بالحاسب الآلي، لن يكون هذا القانون قادرا على أداء الغرض المطلوب وسوف تقف الجهات الأمنية والمحققين مكتوفي الأيدي، في ظل عدم وجود قانون خاص بجرائم الحاسب الآلي أو جرائم تقنية المعلومات، وذلك ما سيتضح من خلال العرض الذي سوف نقدمه للجريمة التي نظرتها محاكم دبي وكيف أن تطبيق هذا القانون

وقانون العقوبات على الجريمة المقدم مرتكبها للمحاكمة لم يكن من السهولة بمكان، وكيف أن القاضي أضطر للاجتهاد والقياس لتوسيع مفهوم النص الجنائي ليتمكن من إدانة المتهم على الرغم من صعوبة ذلك القياس في مجال النص الجنائي، والمحاذير التي تحول دون ذلك الاجتهاد.

- •قانون تنظيم قطاع الإتصالات رقم (3) لسنة 2003 :

صدر قانون تنظيم قطاع الاتصالات ليكون القانون الذي ينظم عمل شركات الاتصالات بالدولة، وينشئ هيئة جديدة تسمى هيئة تنظيم قطاع الاتصالات بالدولة وحددت المادة (12) من هذا القانون مهام وصلاحيات واختصاصات الهيئة بأنها هي السلطة المختصة بالرقابة على قطاع الاتصالات والمرخص لهم، وذلك وفقا لأحكام هذا المرسوم بقانون ولائحته التنفيذية والتعليمات الصادرة عن اللجنة العليا،....الخ).

وورد في المادة رقم (1) من القانون تعريف (لخدمات الاتصالات) بأنها خدمة نقل أو بث أو تحويل أو استقبال من خلال شبكة الاتصالات لأي مما يأتي:

- الاتصالات السلكية واللاسلكية
- الحديث والموسيقى وغيرها من الأصوات
- الصور المرئية
- الإشارات التي تستخدم في البث باستثناء البرامج واذاعتها
- الإشارات المستخدمة في تشغيل والسيطرة على أي آلات أو أجهزة تركيب أو صيانة أو ضبط أو إصلاح أوتغيير أو نقل أو إزالة الأجهزة التي سيتم ربطها أو تكون مرتبطة بشبكة اتصالات عامة
- إنشاء وصيانة وتشغيل شبكات البرق والهاتف والتلكس والدوائر المؤجرة والمعطيات المحلية والدولية والإنترنت والإرسال اللاسلكي
- أي خدمات اتصالات تعتمدها الجنة العليا.

وورد بالباب التاسع من هذا القانون مجموعة مواد تجرم بعض الأفعال وتفرض عقوبات على مخالفة الأحكام والالتزامات التي يفرضها القانون حيث نصت المادة (71) على عقوبة الحبس مدة لاتجاوز سنتين، وبغرامة لاتقل عن خمسين ألف درهم ولا تجاوز مائتي ألف درهم أو بإحدى هاتين العقوبتين كل من يباشر أي من الأنشطة التي نظمها القانون دون الحصول على ترخيص أو إعفاء وفقا لأحكام هذا القانون، أو يقوم متعمدا بتغيير أو اتلاف أو إخفاء أية وثيقة أو معلومة تطلبها اللجنة العليا أو الهيئة أو لم يقم بتعديل أوضاعة وفقا لأحكام هذا المرسوم بقانون خلال المدة المحددة.

كما ورد بالمادة رقم (72) تجريم بعض الأعمال التي يمكن أن تتم عن طريق الخدمات التي تقدمها شركات الاتصالات أو عن طريق أجهزة الاتصالات، حيث فرض القانون في هذه المادة عقوبة الحبس لمدة لا تجاوز سنة وبغرامة لاتقل عن خمسين ألف درهم ولا تجاوز مائتي ألف درهم أو بإحدى هاتين العقوبتين:

1- كل من أقدم أو ساهم في تقديم خدمات اتصالات مخالفة للنظام العام والآداب العامة.
2- كل من استغل أجهزة أو خدمات الاتصالات في الإساءة أو الإزعاج أو إيذاء مشاعر الآخرين أو لغرض آخر غير مشروع.
3- كل من نسخ او افشى أو وزع بدون وجه حق فحوى أي اتصال أو رسالة هاتفية مرسلة من خلال استخدام شبكة اتصالات عامة.
4- كل من قام متعمدا بالدخول غير المشروع لشبكة اتصالات أو قام بتعطيل أي من خدمات الاتصالات .
5- كل من استغل أو استخدم بغير وجه حق أي من خدمات الاتصالات.
6- كل من تنصت على محتوى أو مضمون المكالمات دون إذن مسبق من السلطات القضائية المختصة.

بمتابعة وتمحيص النصوص التي تم استعراضها، فإنه يمكننا القول بأن بعض الجرائم التي يمكن أن تتم عن طريق استخدام شبكة الإنترنت يمكن ملاحقة مرتكبيها بموجب أحكام هذا القانون، حيث ورد النص على أن خدمة (الانترنت) تعتبر من (خدمات الاتصالات) الوارد تعريفها بالمادة الأولى.

كذلك ورد النص صراحة على جرائم محددة وهي(تقديم أو المساهمة في تقديم خدمات اتصالات مخالفة للآداب العامة أو النظام العام) ويندرج تحت هذا المصطلح العديد من الجرائم وخاصة ترويج الصور والمواد الإباحية أو المشاهد الخادشة للحياء أو الدعوة للفجور والرذيلة أو الدعوة لتعكير صفو الأمن واشاعة الفوضى أو تعكير أمن الناس وسكينتهم وتعريض صحتهم للخطر، وهذه الجرائم إذا ارتكبت عن طريق شبكة الإنترنت التي هي خدمة من خدمات الاتصالات فمثل هذه الجرائم يمكن ملاحقة مرتكبيها وفقا لأحكام هذا القانون.

كذلك جريمة تعطيل عمل شبكة الانترنت وهي من الجرائم الخطيرة والمؤثرة يمكن ملاحقة مرتكبيها بموجب نص المادة السابقة حيث ورد في البند رقم(4) النص صراحة على تجريم تعطيل أي من خدمات الاتصالات والتي من ضمنها خدمة الإنترنت.

وحيث أن هذا القانون أعطى الحق للهيئة بالفحص والتدقيق على الأحهزة المستخدمة لتقديم خدمات الاتصالات، فإن من يمتنع عن السماح للهيئة أو للموظفين المختصين بالفحص والتدقيق على الأجهزة التي تكون تحت تصرفه أو الدخول لموقعه فسوف يعرض نفسه للعقوبة المقررة في المادة (74) من هذا المرسوم بقانون وهي الغرامة التي لاتقل عن خمسين ألف درهم ولا تجاوز مائتي ألف درهم. ولاشك أن أجهزة الحاسب الآلي المستخدمة في تلقي خدمة الإنترنت داخلة ضمن حكم هذه المادة، وبالتالي يستطيع الموظفون المختصون ورجال التحقيق فحص أجهزة الحاسب الآلي

التي يعتقدون أنها كانت محلا لنشاط إجرامي بالمخالفة لأحكام هذا القانون والقوانين الأخرى النافذة بالدولة.

ولعله من الأهمية بمكان فى هذا الصدد وبعد استعراض النصوص التي يمكن من خلالها ملاحقة مرتكبي جرائم تقنية المعلومات في القانونين الخاصين بمؤسسة الأمارات للاتصالات، وتنظيم قطاع الاتصالات، أن نشير إلي أن القانون الثاني وهو قانون تنظيم قطاع الاتصالات الصادر في عام 2003 يعتبر معدلا لقانون مؤسسة الإمارات للاتصالات حيث ورد النص صراحة فيه على إلغاء بعض المواد ومن ضمنها المواد الخاصة بالعقوبات، وأصبحت المواد الواردة بقانون تنظيم قطاع الاتصالات هي الواجبة التطبيق على جميع مسائل المخالفات والجرائم المرتكبة من خلال وسائل أو خدمات الاتصالات بالدولة بالإضافة إلي العقوبات الواردة بقانون العقوبات الإتحادي والقوانين الأخرى ذات الصلة.



المبحث الثالث
القصور التشريعى ونمط تعاطى القضاء العربى مع جرائم المعلوماتية

أوجه القصور التشريعي في مصر وغيرها من الدول العربية

إذا حاولنا الوقوف على أوجه القصور التشريعي في كثير من الدول العربية وفى مقدمتها مصر؛ والتي تحول دون الملاحقة الجنائية لمرتكبي الجرائم المعلوماتية يمكننا أن نشير إلى ما يلي :-

(1) إن مبدأ الشرعية الجنائية يفرض عدم جواز التجريم والعقاب عند انتفاء النص. الأمر الذي يمنع مجازاة مرتكبي السلوك الضار أو الخطر على المجتمع بواسطة الحاسوب(الكمبيوتر) أو الإنترنت ؛ طالما أن المشرع الجنائي لم يقم بسن التشريعات اللازمة لإدخال هذا السلوك ضمن دائرة التجريم والعقاب.

ولذا يتعين على المشرعين في سائر الدول العربية مواكبة التطورات التي حدثت في المجمعات العربية ؛ وسن التشريعات اللازمة للتصدي لظاهرة الإجرام المعلوماتي.

وهنا تجدر الإشارة إلى أن المشرع العماني كان له قصب السبق في هذا المضمار؛ حيث نص على تجريم كثير من صور الجرائم المعلوماتية.

(2) يعتبر مبدأ الإقليمية هو المبدأ المهيمن على تطبيق القانون الجنائي من حيث المكان، غير أن هذا المبدأ يفقد صلاحيته للتطبيق بالنسبة للجرائم المعلوماتية، التي تتجاوز حدود المكان، فجرائم الإنترنت عابرة للحدود .

(3) انعدام وجود تصور واضح المعالم للقانون والقضاء تجاه جرائم الانترنت لكونها من الجرائم الحديثة وتلك مشكلة أكثر من كونها ظاهرة، ولانعدام وجود تقاليد بشأنها كما هو الشأن في الجرائم الأخرى، ويساعد على ذلك انعدام وجود مركزية وملكية عبر الانترنت .

(4) رغم صدور عدد من التشريعات العربية بشأن حماية الملكية الفكرية والصناعية التي تضمنت النص على برامج الحاسب واعتبرتها من ضمن المصنفات المحمية في القانون ؛ إلا أن مكافحة الجرائم المعلوماتية في الدول العربية مازالت بلا غطاء تشريعي يحددها ويجرم كافة صورها بخلاف بعض الاستثناءات.

وإذا كان التشريعات العربية – فى الغالب الأعم - قاصرة في مجال ملاحقة صور السلوك الضار والخطر المتعلقة باستخدام الحاسوب (الكمبيوتر) والإنترنت؛ فإن هذا القصور انعكس مردوده على الجانب الإجرائي المتعلق بمكافحة الإجرام المعلوماتي، فلم تصدر تشريعات جنائية إجرائية كافية لتعقب مقترفي هذا الإجرام .

(5) تتعدد مظاهر القصور التشريعي التي يتعين أن تواجه كافة مظاهر السلوك السلبي المتعلقة بتقنية المعلومات . فالتشريعات مازالت ناقصة وقاصرة في المجالات التالية :

- التشريعات الخاصة بالملكية الفكرية فيما يتعلق بأسماء مواقع الانترنت وعناصرها ومحتواها والنشر الإلكتروني وفي حقل التنظيم الصحفي للنشر الإلكتروني.
- تنظيم التجارة الإلكترونية والتشريعات الضريبية التي تغطي الميادين الخاصة بالضريبة في ميدان صناعة البرمجيات والأعمال على الانترنت والتجارة الإلكترونية.
- مقاييس إطلاق التقنية.
- القواعد التشريعية لنقل التكنولوجيا.
- التراخيص والاستثمار والضرائب المتعلقة بتكنولوجيا المعلومات.
- تنظيم حجية ومقبولية مستخرجات الحاسب.
- وسائل الإثبات التقنية والإثبات المدني.

- وتنظيم الصور الإجرامية في ميدان الحاسب والإنترنت .
- أنظمة الدفع النقدي الإلكتروني .
- تنظيم كيفي عمل مقاهي الإنترنت .
- البرمجيات الصناعية .

(6) عدم الاهتمام بالتفتيش على أجهزة الحاسوب (الكمبيوتر)، فالتشريعات العربية – في مجملها - لم تحدد قواعد خاصة للتفتيش على الحاسبات الآلية وكيفية وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها، كما أن الإجراءات الجنائية للجهات القائمة على التفتيش غير حاسمة بشأن مسألة ضبط برامج الحاسب والمعلومات الموجودة بالأجهزة وفقا للشروط الخاصة بإجراءات التفتيش العادية .

(7) إذا كان المحقق مهمته البحث عن الحقيقة، وإذا كان القاضي مهمته هي الفصل فيما يعرض عليه من أقضية ومنازعات، فإن عمل المحقق وعمل القاضي يحتاج إلى بيئة قانونية تساعدهما على أداء وظيفتهما .

الشيء المؤسف أن هذه البيئة القانونية إما غامضة ؛ وإما قاصرة .

ففيما يتعلق بمواطن القصور والغموض، فهى متعددة، ونستلهمها من التساؤلات الآتية:

- هل اعتداءات الأشخاص على الأموال في البيئة الحقيقية يمكن تطبيق مفهومها على اعتداءات المجرم المعلوماتي ؟
- هل المعلومات بذاتها لها قيمة مالية ؟ أم هي تكون كذلك عندما تمثل أصولا أو حقوقا ؟.
- كيف يمكن حماية السر التجاري أو الأسرار الشخصية وبيانات الحياة الخاصة من اعتداءات المجرم المعلوماتي أو المتطفل دون تصريح وإذن ؟.
- وهل هناك معايير تحكم مقدمي خدمات الانترنت بأنواعها ؟.

- ما مدى المسؤولية القانونية في حالة تحميل الملفات الموسيقية من الانترنت بغير موافقة صاحب الموقع ؟؟.
- هل يعتبر النشر الإلكتروني على الانترنت من قبيل النشر الصحفي المنظم في تشريعات الصحافة والمطبوعات ؟ .
- وهل إبرام العقد عبر الانترنت تتوافر فيه سلامة وصحة التعبير عن الإرادة بنفس القدر الذي يوفره التعاقد الكتابي أو الشفهي في مجلس العقد العادي ؟
- وهل توقيع العقود والمراسلات إلكترونيا يتساوى مع توقيعها ورقيا ؟
- هل ما يعتد به من دفوع واحتجاجات بشأن التزامات أطراف التعاقد أو علاقات الدفع التقليدية متاح بذاته أو أقل منه أو أكثر في البيئة الرقمية ؟
- هل لرسائل البريد الإلكتروني حجية في الإثبات ؟ وهل لها ذات قيمة للمراسلات الورقية؟
- هل الانتخاب الإلكتروني هو تصويت صحيح ومقبول لمن اخترناه ممثلا لنا في عالم المكان والجغرافيا؟ .
- هل العلامة التجارية محمية من أن تكون اسم نطاق لطرف آخر ؟
- ماذا عن تصميم الموقع هل ثمة قدرة على منع الآخرين من سرقته واستخدامه؟
- ماذا إن تم ربط موقعك على الانترنت مع موقع لا ترغب في أن يكون بينهما رابط ؟
- ماذا عن فرض المحتوى على المستخدم هل يظل المستخدم عاجزا لا حول له ولا قوة أمام تدفق مواد لا يرغبها أو لا يطلبها على صندوق بريده أو خلال تصفحه المواقع التي يريدها ؟
- هل إغلاق المواقع ذات المحتوى غير المشروع في بعض النظم والمشروع في غيرها تجاوز على ديمقراطية العالم التخيلي ؟

- متى نشأ النزاع أيا كان وصفه أو مصدره فمن هو القاضي الرقمي ؟
- ما هو القانون الذي سيحكم النزاع ؟
- ما المحكمة ومن هو المحكم ؟
- ما هي أخلاق المجتمع الرقمي وقواعد السلوك فيه هل هي ذاتها أخلاق العالم الحقيقي أم ثمة تباين في المفهوم والقيود ؟
- وهل ثمة قدرة للمستخدم أن يطالب بحقوق في مواجهة الطرف الوسيط في كل تعامل أو استخدام نتج عنه مساسا بحق من حقوقه .
- ومن هو حاكم الانترنت وما الدستور الذي يحكمه ومن هو الشرطي الذي يهرع له المستخدم إن تعرض لاعتداء سافر على حقوقه أو بياناته أو محتوى موقعه أو رسائله أو خصوصيته؟ .
- كيفية حماية برامج الحاسب .
- كيفية مقاضاة مزودي خدمة الانترنت على انقطاع الخدمة .
- مراقبة أداء الموظفين عبر البريد الإلكتروني ورسائلهم في بيئة العمل .
- مدى صحة إبرام العقد على الانترنت .
- كيفية حماية مواقع الانترنت .
- هل إرسال رسالة ممازحة عبر البريد الإلكتروني، يمكن ان تشكل جريمة جنائية ؟ وهل يمكن أن ترتب مسئولية مدنية ؟

- بواعث حتمية سد الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية فى مصر والدول العربية :

مما لاشك فيه أن أسباب سد الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية متعددة ؛ وكلها تنبع من كون هذه الجرائم تختلف جملة وتفصيلا عن الجرائم العادية ؛ ولذا يتعين أن يكن تعقبها يراعي هذه الاختلافات .

وعلى كل حال من أهم هذه الأسباب ما يلي:

أولا : سهولة إخفاء الجريمة

الجريمة المعلوماتية - في أغلب الأحوال - تكون مستترة خفية ؛ فعلى سبيل المثال نجد أن اختلاس المال بواسطة التلاعب غير الشرعي ؛ غالبا ما يحاول المختلس تغطيته وستره والتجسس على ملفات البيانات المختزنة ؛ الامر الذي يضعف إلى حد كبير فرصة المجني عليه في إثبات هذا الاختلاس .

ثانيا: نفس الشيء يقال بالنسبة لاختراق قواعد البيانات وتغيير بعض محتوياتها والتخريب المنطقي للأنظمة باستخدام الفيروسات .

ثالثا : نقص خبرة الشرطة وجهات الادعاء والقضاء

رابعا : صعوبة الوصول إلى مرتكبي أغلب الجرائم المعلوماتية

فعلى سبيل المثال : جرائم التزوير عبر الإنترنت تتم دون تحديد شخص مرتكبها أو ضبط المحرر المزور .

خامسا : صعوبة الإثبات

وذلك يرجع إلى :

(1) الطبيعة الخاصة للدليل في الجرائم المعلوماتية، فهو ليس بدليل مرئي يمكن فهمه بمجرد القراءة، ويتمثل – حسب ما تتيحه النظم المعلوماتية من أدلة على الجرائم التي تقع عليها أو بواسطتها - في بيانات غير مرئية لا تفصح عن شخصية معينة عادة .

وتظهر هذه المشكلة بصفة خاصة بالنسبة لجرائم الانترنت مثل الجرائم التي ترتكز على البريد الإلكتروني في ارتكابها ، إذ يكون من الصعب على جهات التحري تحديد مصدر المرسل .

(2) صعوبة الوصول إلى الدليل، وذلك نتيجة قيام كبرى المواقع العالمية على الانترنت بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية

الفنية لمنع التسلل للوصول غير المشروع إليها لتدميرها أو تبديلها أو الإطلاع عليها أو نسخها.

هذا من جهة ؛ ومن جهة أخرى يمكن للمجرم زيادة صعوبة عملية ضبط أي دليل يدينه وذلك من خلال: استخدامه كلمات مرور بعد تخريب الموقع مثلا، أو استخدامه تقنيات التشفير.

(3) سهولة محو الدليل، فالجاني يستطيع أن يتوجه إلى أي "مقهى الانترنت" والدخول على أحد المواقع وإرسال رسالة على البريد الإلكتروني لآخر تحوى عبارات سب وقذف، ثم يقوم بمحو الدليل وإعادة كل شيء كما كان عليه والانصراف إلى حال سبيله .

(4) أدلة الإدانة ذات نوعية مختلفة فهي معنوية الطبيعة، وذلك مثل سجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ والبرمجيات، ولذا فهذه الأدلة تثير أمام القضاء مشكلات عديدة ؛ ولاسيما فيما يتصل بمدى قبولها وحجيتها والمعايير اللازمة لذلك .

سادسا : إحجام الجهات والأشخاص المجني عليهم عن الإبلاغ عن الجرائم المعلوماتية

ويحدث ذلك غالبا بالنسبة للجهات المالية كالمصارف والبنوك ومؤسسات السمسرة؛ إذ أن مجالس إداراتها - في الغالب الأعم - تفضل كتمان أم هذه الجرائم تفاديا للآثار السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية تجاهها؛ إذ قد يؤدي ذلك إلى تضاؤل الثقة فيها من جانب المتعاملين معها.

سابعا : صعوبات شديدة في ضبط وتوصيف جرائم المعلوماتية

لا مراء في أن رجال الضبطية القضائية والمحققين والقضاة يصادفون صعوبات جمة فيما يتعلق بإجراءات ضبط الجرائم المعلوماتية ؛ وإضفاء الوصف القانوني المناسب على الوقائع المتعلقة بهذه الجرائم.

ولعل مرد ذلك يرجع إلى الطبيعة الخاصة لهذه الجرائم . فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود.

ثامنا : تصادم التفتيش عن الأدلة في الجرائم المعلوماتية مع الحق في الخصوصية المعلوماتية

وذلك لأن هذا لتفتيش يتم – غالبا - على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، الأمر الذي قد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة ؛ نظرا لشيوع التشبيك بين الحواسيب وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول.

ولاشك في أن امتداد التفتيش إلى نظم غير النظام محل الاشتباه قد يمس – في الصميم - حقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش .

تاسعا : فكرة الاختصاص والطبيعة الدولية للجرائم المعلوماتية

الجرائم المعلوماتية تتم – في الغالب الأعم- بأفعال ترتكب من قبل أشخاص من خارج الحدود كما أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود ، الأمر الذي

يثير التساؤل حول الإختصاص القضائي بهذه الجرائم ؛ علاوة على أن امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود ؛ أمر يحتاج إلى تعاون دولي شامل يستهدف تحقيق مكافحة هذه الجرائم ؛ مع احترام السيادة الوطنية للدول المعنية .

أمثلة تطبيقية لنمط تعاطى القضاء العربي مع الجرائم الإلكترونية:

1- مثال تطبيقى من دولة الإمارات لجريمة الكترونية نظرت أمام القضاء الوطنى قبل صدور قانون مكافحة جرائم تقنية المعلومات:

وقعت الجريمة عبر (شبكة الإنترنت) في دولة الإمارات قبل صدور قانون مكافحة جرائم تقنية المعلومات رقم 2 لسنة 2006، حيث تم القبض على مرتكبها وتقديمه للعدالة بموجب قانون العقوبات الإتحادي، وصدر حكم المحكمة الأبتدائيه ببراءته من التهمة لعدم وجود نص واضح يجرم الفعل الذي قام به، وفي محكمة الاستئناف تعدل الحكم إلي إدانة المتهم وتأيد الحكم من محكمة التمييز.

وتثور فى هذا الصدد عدة تساؤلات منها:

- لماذا لم تستطع المحكمة الابتدائية إدانة المتهم؟
- وكيف توصلت محكمة الاستئناف الي إدانته ؟
- وماذا قالت محكمة التمييز عن الحكم، وكيف بررت تأييدها له، في الرد على أوجه الطعن الموجه له من الدفاع؟
- وكيف أوحت محكمة التمييز بأن هناك حاجة إلي نصوص قانونيه تعالج جرائم الحاسب الآلي الحديثة في الدولة؟

وللاجابة على هذه التساؤلات كان من المهم أن نستعرض هذه القضية ونسبر أغوارها فيما يلى:

1- اتهمت النيابة العامة المدعو(.....) في الجنحة رقم **2000/5883** :

بأنه في يوم 2000/6/21، استغل وأساء استخدام خدمة من خدمات مؤسسة الإمارات للاتصالات (خدمة الإنترنت) وذلك لأغراض غير مشروعة بأن زود الحاسب الآلي الذي يستخدمه والمتصل بهذه الخدمة ببرنامج قرصنة تمكن من خلاله من كسر الكلمات السرية الخاصة ببعض موظفي مؤسسة

الامارات للاتصالات والدخول إلى الأماكن غير المصرح بها لمشتركي الشبكة ونسخ بعض الكلمات الخاصة بالكلمات السرية ورسائل البريد الالكتروني لموظفي مؤسسة الامارات للاتصالات مع علمه بذلك.

2- فض المتهم عددا من الرسائل الواردة إلى بعض موظفي مؤسسة الإمارات للاتصالات والمسجلة على البريد الالكتروني للمؤسسة:

وذلك بأن قام بكسر الكلمات التي تحول دون علم و اطلاع الغير عليها ونسخ صورا منها احتفظ بها على جهاز الحاسب الآلي الخاص به وطلبت النيابة معاقبته طبقا لنص المادة 7/46 من القانون رقم (91/1) في شأن مؤسسة الاتصالات و المادة 380 عقوبات وادعت المؤسسة مدنيا قبل المتهم طالبة الحكم بالزامه بمبلغ 2.835000 درهم على سبيل التعويض.

3- وبتاريخ **2001/7/1** حكمت محكمة أول درجة ببراءة المتهم من التهمة الثانية،

وهي تهمة فض الرسائل المؤثمة بموجب قانون العقوبات، وكان سند البراءة أن القاضي الإبتدائي اعتبر ان الرسالة الإلكترونية الواردة بالإيميل، شي مغاير للرسالة العادية المكتوبة، وأن النص الجنائي فرض الحماية على هذه الأخيره فقط، ذلك أنه عند ما صدر قانون العقوبات لم يكن هناك شي يسمى بالرسالة عبر الإيميل، وتحترز من استخدام القياس في مجال النص الجنائي التزاما بقاعدة الشرعية الجنائية، ولعدم وجود مباديء من المحكمة العليا في هذا الشأن.

وأدانت المحكمة المتهم عن التهمة الأولى وهي إساءة واستغلال خدمة من خدمات الاتصالات وطبقت عليه العقوبة الواردة بقانون مؤسسة الاتصالات وقامت بتغريمه عشرة آلاف درهم عن هذه التهمة وبإحالة الدعوى المدنية إلى المحكمة المدنية المختصة .

4- لم يرتض المحكوم عليه و النيابة العامة الحكم فطعنا عليه بالاستئناف:

فحكمت الاستئناف بالغاء ما قضى به الحكم المستأنف و القضاء مجددا بتغريم المتهم عشرة آلاف درهم عن التهمتين المسندتين إليه مع مصادرة المضبوطات بعد أن أعملت قواعد الارتباط بين التهمتين أي أن محكمة الاستئناف أدانته عن تهمة فض الرسائل الإلكترونية وقاستها على الرسائل العادية، وتوسعت في مفهوم النص.

طعن المحكوم عليه على الحكم بطريق التمييز ونعى عليه بأن قد شابه القصور في التسبيب والفساد في الاستدلال والخطأ في تطبيق القانون؛ ذلك أنه لا جريمة ولا عقوبة إلا بنص والمشرع هو الذي يضع النصوص التجريمية وقد اخطأ الحكم المطعون فيه إذ استند في ادانة الطاعن الى المادة 5/46 من القانون رقم 1991/1 في شأن مؤسسة الإمارات للاتصالات إذ كيف الأعمال المسندة إلى الطاعن بأنها جنحة استخدام خدمة الإنترنت دون بيان السند القانوني في تجريم هذه الأعمال وعدم مشروعيتها كما أن القانون المذكور لا يمكن تطبيقه على الواقعة المسندة إلى الطاعن لأنه لا يشتمل على أي نصوص أو مواد متعلقة بخدمة الإنترنت أو الجرائم التي تترتب على استخدامه نظرا لأن هذا القانون قد صدر في تاريخ سابق على وجود نظام الإنترنت في الدولة وأخطأ الحكم في إدانة الطاعن عن التهمة الثانية إعمالا للمادة 380 عقوبات التي تعاقب على فض الرسائل و البرقيات دون إذن صاحبها و الأعمال المسندة إلى الطاعن تخرج تماما عن نطاق هذه المادة ولا يجوز القياس عليها إذ هي تتعلق بالرسائل و البرقيات المكتوبة ولم يوضع الحكم ما هي الطرق المصرح باستخدامها عند استخدام الانترنت والطرق غير المصرح بها وسند ذلك في القانون كما جاء بأسباب الحكم أن

الطاعن دخل إلى المواقع المحظور دخولها دون أن يبين سند هذا الحظر والنص القانوني المستند إليه وقد تخلف ركن القصد الجنائي لدى الطاعن إذ انه لم يقم بالإطلاع على الرسائل البريدية الخاصة بموظفي الهيئة عمدا بل اطلع على بعض الرسائل الموجودة في جهاز عام دخل إليه مصادفة بدلالة أقوال الشاهد مدير التشغيل بشبكة الإنترنت التي تفيد أن الطاعن لم يدخل على صندوق بريد خاص بأي من موظفي المؤسسة و إنما دخل الجهاز الخاص بارسال الرسائل البريدية وهو لا يشكل جريمة معاقب عليها مما يعيب الحكم بما يستوجب نقضه.

5- تأييد محكمة التمييز لإدانة المتهم وتبرير الحكم :

وقد جاء فى قضاء محكمة التمييز أن التهمتين تحقق ثبوتهما في حق الطاعن بأدلة سائغة لها معينها الصحيح من أوراق الدعوى ومن شأنها أن تؤدى إلي ما رتبه الحكم عليها مستمدة مما شهد به (الشهود) وتقرير المختبر الجنائي و المضبوطات واعتراف المتهم بتحقيقات النيابة العامة... لما كان ذلك، ولئن كان الأصل أنه يجب التحرز في تفسير القوانين الجزائية والتزام جانب الدقة في ذلك وعدم تحميل عباراتها فوق ما تحتمل إلا وأنه في حالة غموض النص فإن ذلك لا يحول دون تفسيره على هدي مما يستخلص من مقصد الشارع وما يحقق الغاية التي تغياها من تقريره كما أن لمحكمة الموضوع تكييف بعض الأمور غير المحددة في القانون على أن يكون هذا التكييف خاضعا لرقابة محكمة التمييز ومن المقرر أيضا أنه إذا ورد في النص التشريعي لفظ مطلق ولم يقم الدليل على تقييده، فقد أفاد ثبوت الحكم على اطلاقه ولما كانت المادة 46 من القانون رقم 1991/1 تنص على عقاب كل من يستخدم الأجهزة أو الخدمات أو التسهيلات التي تقدمها المؤسسة في الازعاج إو إيذاء مشاعر الآخرين او أي غرض آخر غير مشروع وكانت

هذه العبارة قد وردت على سبيل الاطلاق في مجال بيان الأعمال المؤثمة ما مفاده شمول الحظر لكل فعل غير مشروع في نطاق أعمالها أيا كانت طبيعته طالما خرج عن الغرض المحدد له في استخدام الشبكة طبقا للنصوص المستخدم عليها في المادة 12 من القانون و المعاقب عليها في المادة 45 منه .... لما كان ذلك وكان الحكم المطعون فيه وفي حدود السلطة التقديرية وفي التفسير و التكييف قد أورد في أسبابه ان الغرض غير المشروع على اطلاق عبارة النص يشمل كل فعل او امتناع عن فعل تجرمه القوانين أو اللوائح وأن ما قام به المتهم باعترافه من اختراقه بشبكة الاتصالات (الإنترنت) التابعة لمؤسسة الإمارات، مستخدما برامج للبحث عن الثغرات واستطاع بذلك الحصول على كلمات السر لبعض المواقع المحظورعلى غير موظفي المؤسسة الدخول إليها و قام بفك شفرة بعض الأجهزة ونسخ بعض الملفات وهو يعلم بحظر ذلك لغير موظفي المؤسسة المرخص لهم، كما قام بفك رسائل البريد الإكتروني لبعض الموظفين ونقلها إلى جهاز الحاسب الآلي الخاص به مما يشكل استغلال للشبكة لغرض غير مشروع يوقعه تحت طائلة العقاب وهي أسباب سائغة تتفق وصحيح القانون وتتوافر بها كافة الإركان القانونية للتهمة الأولى المسندة إلى الطاعن مما يكون معه منعاه -في هذا الخصوص- غير سديد.... لما كان ذلك وكانت خدمة الإنترنت تدخل ضمن الخدمات التي تقدمها مؤسسة مع الاتصالات وتخضع لأحكام القانون رقم 1991/1 الخاص بمؤسسة الاتصالات، فإن ذلك لا يتعارض مع عدم صدور تشريع خاص بخدمات الإنترنت ويكون نعى الطاعن في هذا الصدد غير مقبول .. لما كان ذلك وكانت المادة 380 عقوبات تعاقب على فض الرسائل و البرقيات بغير رضاء من ارسلت إليه وهو ما يسري على البرقيات سواء كانت مكتوبة أو مرئية أو مسموعة دون قصرها على

المحررات المكتوبة حسبما يدعي الطاعن وإذ دان الحكم المطعون فيه الطاعن لاستخدامه خدمة الإنترنت لهذا الغرض غير المشروع، وهو الاطلاع على الرسائل الخاصة دون رضاء أصحابها فإنه يكون قد أصاب صحيح القانون ويكون نعى الطاعن في هذا الخصوص في غير محله ... لما كان ما تقدم فإن الطعن برمته يكون على غير أساس متعين الرفض موضوعا، وعليه حكمت المحكمة برفض الطعن.

وبالنظر الي عبارات محكمة التمييز فإننا نجد أنها اشارت الي غموض النص، وأنه يجب التحرز في تفسير النصوص الجنائية وعدم تحميل عباراتها ما لاتحتمل، وأنها أدانت المتهم بالنظر إلي الغاية التي تغياها المشرع، وفسرت النص في ضوء تلك الغاية والمقصد المشروع.

وغنى عن البيان أن عبارات محكمة التمييز في تبريرها للحكم توحي بأن هناك حاجة لإزالة الغموض وعدم ترك مسائل تجريم الأعمال المتصلة بالحاسب الآلي وشبكة الإنترنت للاجتهاد والقياس في تفسير النصوص للتمكن من إدانة المتهمين، وأولئك الذين ارتكبو أعمالا قد تكون نتائجها وخيمة، لاتقدر بثمن، وتضر بمصالح شخصية، وقومية يحظر المساس بها، وأنه لابد من سن تشريعات صريحة ومتخصصة في مجال الجريمة الحديثة جريمة تقنية المعلومات.

2- عرض لجريمة أخرى وقعت في الإمارات بعد صدور قانون مكافحة جرائم تقنية المعلومات رقم 2006/2:

وقعت هذه الجريمة في شهر يونيو من العام 2006 بدبي وقدمت النيابة العامة إثنين من المتهمين فيها للمحاكمة - وهي أول جريمة تقدم استنادا لقانون مكافحة جرائم المعلومات الإماراتى ويدان مرتكبها- واتهمت النيابة العامة بدبي المتهم الأول بأنه (توصل عن طريق الشبكة المعلوماتيه إلي

الاستيلاء على مال منقول (عدد خمس تذاكر سفر) عائد لشركة سفريات وسياحة بدبي بطريقة إحتيالية وباتخاذ صفة غير صحيحة بأن تمكن من دخول موقع الشركة الإلكتروني عن طريق استخدام الرقم السري واسم المستخدم (الخاصين بالمتهم الثاني) وهو أحد موظفي الشركة وكان ذلك من شأنه خداع الشركة وحملها على تسليم تذاكر السفر .
واتهمت النيابة الثاني بأنه اشترك بالاتفاق والمساعدة مع المتهم الأول بارتكاب الجريمة المبينة في الوصف السابق فوقعت الجريمة بناء على ذلك الاتفاق والمساعدة، كما اتهمته بأنه بحكم عمله لدى الشركة بمهنة بائع تذاكر افشى سر مهنته (الرقم السري واسم المستخدم) في غير الأحوال المصرح بها قانونا واستعمله لمصلحته الخاصة ومصلحة المتهم الأول دون إذن من صاحب الشأن.
وطلبت النيابة عقابهما بالمواد (1،10،23،25) من القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات والمادة 379 من قانون العقوبات الاتحادي.
وقد دافع المتهم الأول عن التهمة الموجهة له بأنه لم يكن يقصد الاحتيال وقد ردت المحكمة هذا الدفاع بأن المتهم قد اتفق مع المتهم الثاني (الموظف بالشركة الهارب) وحصل منه على الرقم السري واسم المستخدم الخاصين به، وقام في أزمنة مختلفة باستخدامها عن طريق الدخول على موقع الشركة وتمكن من الحصول على التذاكر بإعترافه، مع أنه ليس له صفة الدخول ولايحق له استخدام الرقم السري واسم المستخدم، مما يشكل فعله طريقة إحتياليه بإتخاذ صفة غير صحيحة ليتمكن من الدخول للموقع وكان من شأن ذلك خداع الشركة وحملها على تسليم تذاكر السفر المبينة بالأوراق.
وقد أدانتهما المحكمة طبقا للمادة 212 من قانون الأجراءات الجزائية الإماراتى والمواد(1،10،23،25) من قانون جرائم تقنية المعلومات والمادة 379

من قانون العقوبات وحكمت على المتهم الأول بالحبس لمدة شهرين وابعاده عن البلاد، وعلى المتهم الثاني بالحبس لمدة سنة واحدة وابعاده عن البلاد.

وقد أعملت المحكمة قواعد الارتباط المقررة في القانون بالنسبة للتهم الموجهه للمتهم الثاني وعاقبته بالعقوبة المقررة للجريمة الأشد، كما أنها طبقت أحكام المواد 99 و100 من قانون العقوبات وعاملت المتهم الأول بقسط من الرأفة لظروف الدعوى وتنازل المجني عليها(الشركة).



الفصل الرابع
الجرائم الإلكترونية فى أوروبا
والولايات المتحدة الأمريكية ووسائل مواجهتها

يتناول هذا الفصل الجريمة الإلكترونية فى أوروبا وأمريكا عبر أربعة مباحث، انفرد المبحث الأول بالحديث عن تطور حجم خسائر الجرائم المعلوماتية فى الدول الغربية أما المبحث الثانى فقد اختص بتناول الجريمة الالكترونية بين التشريع والقضاء فى الدول الغربية فيما ركز المبحث الثالث على موقف التشريعات اللاتينية من جريمة سرقة المعلومات وأخيرا جاء المبحث الرابع متحدثا عن آليات مكافحة الجريمة الإلكترونية فى الدول الغربية.



المبحث الأول
تطور حجم خسائر الجرائم المعلوماتية فى الدول الغربية

يصعب تقدير حجم الخسائر المترتبة على جرائم نظم المعلومات[1] والسبب في ذلك الرقم الأسود الذي يسيطر على هذا النوع من الإجرام علاوة على الموقف السلبي للمجني عليهم في هذه الجرائم، ولصعوبة اكتشاف الجريمة المعلوماتية[2].

لذا فإنه من الصعوبة تقدير حجم الخسائر الناشئة عن هذه الجرائم[3] كما تشير بذلك الأبحاث التي أجريت في هذا الشأن سواء في فرنسا أو الولايات المتحدة الأمريكية أو إنجلترا.

---

(1) المخربون : يقوم المخربون باستخدام بعض الوسائل الأوتوماتيكية لاكتشاف نقاط الضعف في نظم الكمبيوتر بغرض زرع البرنامج المدمر في تلك النظم، ويظل هذا البرنامج كامنا حتى يحين موعد الهجوم المحدد.
فإذا ما قام المخربون بزرع البرنامج المذكور عبر جهاز كمبيوتر خاص بشخص آخر فإن ذلك يزيد من صعوبة تعقبهم.
راجع في ذلك:

Dr: Linda Volonino. Cybet Terrorism. Op. cit.

(2) Bertin et Lambertie, la protection du logiciel, enjeux juridiques et economiques L.G.D.J. 1985, p. 30

(3) وتجدر الإشارة في هذا الصدد إلى أن إحجام ضحايا الجرائم المعلوماتية عن الإبلاغ عن الجرائم المرتكبة في حقهم – سواء لخوفهم من الفضيحة أو لاعتقادهم بعدم قدرة الشرطة على التعامل مع مثل هذه الجرائم، = = أو لعدم درايتهم من حيث المبدأ- لوقوع مثل هذه الجرائم – أن هذا الإحجام يؤدي إلى فرار المجرمين من العقاب كما أنه يترك وحدات جرائم الكمبيوتر الشرطية التي تتمتع بكفاءة عالية دون عمل يذكر ومن هنا يظل النطاق الحقيقي لجرائم الكمبيوتر : حجمها، طبيعتها ومداها وتهديداتها – تظل كلها أمور غامضة، انظر:

HACKER CRACK DOWN Law and Disorder on the Electronic Frontier b : Bruce sterling p. 168. 1994.

- تقدير خسائر الجرائم المعلوماتية في الولايات المتحدة الأمريكية:

أجرى المكتب الأعلى للإحصاء la general Accounting office عام 1976 تحقيقا بخصوص ظاهرة الغش في الأنظمة المعلوماتية الخاصة بالحكومة الفيدرالية، وجاءت نتيجته على النحو التالي :

- 40% حالات اختلاس أشياء مختزنة ترتب عليها خسارة قدرت بحوالي 57.000 دولار.
- 39% حالات اختلاس أموال تسببت في خسارة قدرت بـ 34.000 دولار.
- 12% حالات تعديل غير مسموح به في البيانات.
- 6% حالات استخدام غير مسموح به للأنظمة المعلوماتية.
- 3% حالات اتلاف.

فغالبية أفعال الغش ارتكبت عن طريق إدخال بيانات مصطنعة 62%. ثم يلي ذلك الاستعمال غير المشروع للوسائل المعلوماتية "25%" ويأتي في المرتبة الثالثة تعديل المعالجات المعلوماتية "23%" وأخيرا اختلاس الوثائق الصادرة عن الحساب الآلي "17%"[1].

وأجريت دراسة عام 1984، بواسطة المعهد الأمريكي للتصديق على الإحصاء العام بخصوص الغش المعلوماتي في البنوك وشركات التأمين والتي انتهت إلى أنه في غالبية الحالات "60%" يتحقق الغش عن طريق التلاعب في الصفقات، إما بخلق معلومات مصطنعة أو اتلاف أو تعديل بيانات حقيقية، وفي ثلث الحالات عن طريق التعديل في مناطق تسجيل الملفات، وأن استمرار فعل الغش يرتبط بالوضع الوظيفي لمرتكبه. وهكذا

---

(1) انظر د. محمد سامي الشوا، - ثورة المعلومات وإنعكاساتها على قانون العقوبات، ص 25.

فإن 41% من حالات الغش بوشرت عن طريق مستخدمين استمرت لمدة أقل من سنة واحدة، 15% من تلك الحالات نفذت بواسطة مسئولين استمرت لمدة أكثر من سنة، ويتوافر لهذه الفئة الأخيرة إمكانيات لإخفاء أفعالهم، ويتطابق الوضع الوظيفي والمبالغ المتحصلة من أفعال الغش حيث أن 59 من حالات الغش والتي قدرت بأقل من 25.000 دولار قد تم ارتكابها بواسطة مستخدمين في البنوك و85% في شركات التأمين، بينما نسبت أفعال الغش التي تجاوزت 1000.000 دولار إلى المستخدمين الذين يشغلون مراكز متقدمة[1].

وباشر الاتحاد الأمريكي للمحامين تحقيقا عام 1984 على 283 منشأة ومؤسسة كبري، وتبين أن ثلثيهما وقعتا ضحية لظاهرة الغش المعلومات بدرجات متفاوتة. كما أظهر التحقيق، أنه عندما يكون الحاسب الآلي موضوعا للجريمة، فإن ثماني منشآت من عشر يعتبرون أن محو أو إتلاف البيانات يمثل النمط الأكثر خطورة لهذه الظاهرة، ونفس الأمر بالنسبة لسرقة أو إتلاف البرامج، وعلى النقيض بالنسبة لسرقة أو إتلاف المعدات المادية فهي تبدو على وجه التحديد اقل خطورة.

ويستحيل نسبيا معرفة إجمالي الخسائر التي لحقت بالمنشآت الأمريكية ووفقا لتقدير الاتحاد الأمريكي للمحامين، فإن ربع هذه المنشآت قد عانت من خسائر في العام السابق على إجراء التحقيق، تفاوتت من 145 إلى 730 مليون دولار، وهذا يعكس تباينا واضحا في الخسارة من منشأة أخرى وعلى وجه العموم فقد قدرت بأقل من 100.000 دولار بالنسبة لـ 20% من هذه المنشآت. وقدرت بأكثر من مليون دولار لـ 4% منها، وأن 28% من هذه المنشآت لم تعلم مقدار الخسارة التي لحقت بها من أثر الغش المعلوماتي[2].

---

(1) المرجع السابق.

(2) المرجع السابق.

- تقدير حجم خسائر الجرائم المعلوماتية في إنجلترا:

قدر اتحاد الصناعات الإنجليزية عام 1976 الخسائر الناشئة عن الغش المعلوماتي بمبلغ يتراوح ما بين 25 إلى 30 مليون جنيه إسترليني في السنة.

وتوضح الدراسة التي قام بها K. Wong على 95 حالة غش معلوماتي أن متوسط الخسارة فيها بلغ 30.000 جنيها إسترلينيا. كما أبانت عن أن سرقة المعدات المادية ولاسيما "الحاسبات الآلية الميكروية" والحرائق العمدية والإتلاف لا تمثل كل منها سوي 30% من الحالات محل الدراسة. ومع ذلك فإن خسائرها كانت مرتفعة جدا.

وبالنسبة لسرقة المعلومات والبرامج "وتمثل 15% من الحالات"، فهي تباشر بصفة أساسية عندما يحل المستخدمون محل الإجراء، وأن إتلاف التجهيزات غالبا ما يتسبب عنه الطاقم المسئول عن تشغيل وتخزين الدعائم الممغنطة، ولكن بالنسبة لإتلاف وظيفة النظام " bombes logiques 8%" فهو من صنع المبرمجين أو أصحاب البرامج. ويمثل انتهاك الأنظمة المعلوماتية بغرض الحصول على معلومات أو خدمات مجانية نسبة تقدر بحوالي العشر، ولكن هذا النمط من الإجرام سيتضاعف بسبب انتشار الحاسبات الميكروية المنزلية[1].

- تقدير خسائر الجرائم المعلوماتية في فرنسا:

ارتفع معدل الخسائر الناتجة عن المعلوماتية في فرنسا حيث بلغت عام 1986 وفقا لإحصاء الجمعية العمومية لشركات التأمين ضد الحرائق والمخاطر المختلفة APSAIRO حوالي 7.3 مليار فرنك فرنسي، ويرجع 46% منها إلى الأفعال الإجرامية و 30% إلى المخاطر العارضة و24% إلى الأخطاء.

(1) المرجع السابق ص ص 27 – 28 .

ويتبين من تحليل الخسائر المرتبطة بجرائم المعلومات في فرنسا أن 60% منها يتعلق بالبرامج، ويتركز الغش في معظم هذه الحالات في اتفاقات غير مشروعة (35%) واستغلال الأعطال القائمة 10% وتضليل البرامج 9% ومن ناحية التشغيل فإن 25% من الخسائر ترجع إلى تعديل الإجراءات والملفات والسهو المتعمد ونقل البيانات.

وقد تضاعفت خسائر سرقة البرامج المنطقية ذو النمط الواحد في الفترة ما بين 1984 إلى 1985 وفقا لتقدير وكالة حماية البرامج لتصل إلى 1.12 مليار فرنك ويرجع 43% من هذه الخسائر إلى سرقة أدوات البرامج المنطقة ذو النمط الواحد "كبرامج الفائدة الخاصة بالتصنيف والمعاونة في تصميم برامج وإدارات البيانات والأمن وصيانة البرامج، و 30% للبرامج المنطقية التطبيقية ذو النمط الواحد الخاصة بالسداد والمحاسبة وإدارة الوثائق، 17% للبرامج المنطقية الأساسية ذو النمط الواحد الخاصة بأنظمة التشغيل، وقدرت خسائر الألعاب بحوالي 10%. ويشهد معدل الخسائر في مجال صفقات الإنتاج وشركات الخدمات والمنشآت الناشرة للبرامج ارتفاعا ملحوظا حيث وصلت الخسائر إلى 19% في عام 1985، 50% منها للحاسب الآلي الميكروي، 11% للأنظمة المتوسطة والكبيرة[1].

- المجالات المستهدفة في مجال جرائم سرقة نظم المعلومات:

يتركز الاتجاه الأساسي لجرائم نظم المعلومات وفقا لتحقيق أجرته مجلة Ressources informatiqes تبين أن:

- 19 % من أفعال الغش المعلوماتي تستهدف البنوك.
- 16% للإدارة.
- 10% للإنتاج الصناعي.
- 10% المعلومات.

(1) انظر في ذلك المرجع السابق ص ص 20-21 .

ثم يلي ذلك شركات التأمين والشركات الخاصة. وفي واقع الأمر أن جرائم نظم المعلومات تستهدف في المقام الأول المؤسســات المالية والتي تتحكم في القيم الرأسمالية.

ويمكن التأكيد من جهة أخرى على أن المعلومات قد صارت أحد المصالح الأساسية المستهدفة بعد النفوذ حيث أصبحت هي المنفذ إلى اقتصاد السوق وقد بني على أساسها بصناعة المعلومات.

وقد نما إلى جوار "السوق الشرعي للمعلومات" marche legalde information السوق السوداء للمعلومات وفيه تتم مقايضة وبيع المعلومات المسروقة أو المقتبسة من أصحابها الحقيقيين والشرعيين، ويرتبط هذا النوع من الإجرام إذن بالجزء الأعظم للأنشطة الاقتصادية والاجتماعية للمجتمع. ويمكن تصوره بالنسبة للمعلومات الآتية :

أ-المعلومات المالية :

حيث تمس هذه الظاهرة المركز الحسابي والإداري وتنقلات الأموال والاستثمارات سواء في المنشآت العامة أو الخاصة.

ب-المعلومات التجارية والصناعية :

حيث تستهدف هذه الظاهرة الدراسات الخاصة بالأسواق ومشروعات الاستثمار والتصنيع والإنتاج والتجارة والتوزيع والأسعار ومراكز البيع والقطاع الصناعي للإنتاج.

جـ-المعلومات الشخصية :

وهي تلك المختزنة في ذاكرات الحاسبات الآلية للبنوك وشركات التأمين ولدي المحامين والمستشفيات وأقسام الشرطة والأحزاب والنقابات. وقد تهدد هذه الاعتداءات مباشرة قدسية وسرية الحياة الخاصة أو الحرية النقابية والسياسية ... إلخ.

د- المعلومات العسكرية :

والتي تتمثل في أسرار الدولة والمشروعات النووية والتصنيع الحديث للأسلحة ...إلخ.

ويبدو أن هذه المعلومات الأخيرة هي الأكثر رواجا في "سوق المعلومات السوداء".

ويمكن الاستئثار بهذه المعلومات عن طريق معالجتها معالجة معلوماتية farun traitement in formatique ومؤدي ذلك أن مجرد المعالجة المعلوماتية يسمح بإدارتها على نحو جيد وعلى الرغم من المخاطر التي يمكن أن تتعرض لهذا هذه الإدارة الآلية.

وتجدر الإشارة إلى أن هذه المعلومات من خلال تداولها واستخدامها عبر الحاسب الآلي أصبحت عرضة لتلف والدمار، وبالتالي لا يستطيع المشتري الاستفادة منها سواء كان ذلك بسبب يرجع إلى البائع أو الغير من خلال ما يعرف بفيروس الحاسب الآلي. وفي ظل التطور الهائل المحسوس في عصرنا الحالي من اتساع درجة الاعتماد على استخدام المعلومات المبرمجة من خلال الحاسبات الآلية وما قد ينشأ عن ذلك من أضرار قد تلحق بالمعلومات نفسها إذا ما أصابها التلف والضرر من جراء فيروسات الحاسبات الآلية أو الضرر الذي يلحق بمستخدميها، فهنا بالتأكيد ستقوم المسئولية تجاه الشخص الذي تسبب في هذا الضرر ويجب عليه التعويض عما لحق بالآخرين من ضرر.



المبحث الثانى

الجريمة الالكترونية بين التشريع والقضاء فى الدول الغربية

تعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام (1973م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها .

وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصة بحماية أنظمة الحاسب الآلي (1976م – 1985م)، وفي عام (1985م) حدد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب. وفي عام (1986م) صدر قانونا تشريعا يحمل الرقم (1213) عرف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي.

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام (1981م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى.

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت حيث عدلت في عام (1985م) قانونها الجنائي بحيث شمل قوانين

خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي.

وفي عام (1985م) سنت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها .

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (1988م) القانون رقم (19-88) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها.

أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التنصت على المكالمات الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام.

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والانترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج.

وغير ذلك من الدول الاوربية هولندا والمجر وبولندا ...كل الدول عدلت من القوانين الجنائية ليتم ادخال الجرائم المعلوماتيه فى اطار قانونى ويتم

تجريم كل ما يشملها من عمليات احتيال ونصب وملكيه فكرية واختراق اجهزة الاخرين وما الى ذلك،،،، ولكن مع الاسف على المستوي العربي لم تقم دولة عربية بسن قوانين خاصة بالحاسب الالي والانترنت وكذا الحال بالنسبة لمملكة البحرين فلا توجد قوانين خاصة بجرائم الإنترنت، وان وجد نص قريب من الفعل المرتكب فان العقوبة المنصوص عليها لا تتلاءم وحجم الأضرار المترتبة على جريمة الإنترنت.

- نماذج لجرائم معلوماتية ارتكبت فى الدول الغربية:

(1)- في بنك لويدز في أمستردام، قام شاب عمره 26 سنة بتحويل مبلغ 8.4 مليون دولار عبر نظام الحوالات العالمية من فرع هذا البنك في نيويورك إلى حساب في بنك آخر في سويسرا. واعتقلت الشرطة في إحدى مدن ولاية أوريجن الأمريكية شابا عاطلا عن العمل عمره 26 عاما استخدم أحد مواقع الدردشة على الإنترنت لتنظيم انتحار جماعي فيما يسمى بعيد الحب هذا العام لمن لم يوفق في حياته العاطفية.

(2)- روبر مورس شاب أمريكي يبلغ من العمر 23 عاما أطلق فيروسا باسمه دمر 6 آلاف نظام عبر الإنترنت بينها أجهزة عدد من المؤسسات الحكومية بخسائر بلغت مئة مليون دولار، عوقب على إثرها بالسجن لمدة 3 سنوات.

(3)- أما تيموثي ألن ليود (35 عاما) فهو مصمم ومبرمج فصل من عمله، فما كان منه إلا أن أطلق قنبلة إلكترونية ألغت كافة التصاميم وبرامج الإنتاج لأحد أكبر مصانع التقنية العالية في نيوجرسي التي تعمل لحساب وكالة الفضاء NASA والبحرية الأمريكية.

(4)- الشاب الفرنسي جان كلود، خلافا لسلوك العصابات، فرغم أنه استطاع تصميم بطاقة صرف آلي وسحب بها مبالغ من أحد البنوك إلا أنه ذهب إلى البنك وأعاد إليه المبالغ وأخبرهم أنه فعل ذلك ليؤكد لهم أن نظام

الحماية في بطاقات الصرف الخاصة بالبنك ضعيف ويمكن اختراقه، إلا أن ذلك لم يمنع الشرطة الفرنسية من إلقاء القبض عليه ومحاكمته. الأمر نفسه فعلته مجموعة من الشباب الأمريكي أطلقوا على أنفسهم "الجحيم العالمي" إذ تمكنوا من اختراق مواقع البيت الأبيض، والمباحث الفيدرالية، والجيش، ووزارة الداخلية؛ لكنهم لم يخربوا تلك المواقع، بل اقتصر دورهم على إثبات ضعف نظام الحماية في تلك المواقع، إلا أنهم حوكموا أيضا. وقبل 5 سنوات ألقت السلطات الإسرائيلية القبض على شابين شقيقين ضريرين من الفلسطينيين ووجهت إليهما تهمة اختراق مواقع وزارة الدفاع الإسرائيلية.

وفي واقع الأمر أن لغة الأرقام تؤكد أننا أمام تحد خطير، فخسائر الشركات الصناعية والتجارية في بريطانيا من جرائم الإنترنت تجاوزت 1.1 مليار جنيه استرليني. أما مكتب التحقيقات الفيدرالية الأمريكية (FBI) فقدر حجم الخسائر الناجمة عن الجرائم الإلكترونية في أمريكا بحوالي 10 مليارات دولار سنويا عام 1998م، ارتفعت إلى 14 مليار عام 2004م.

والمثير أن 17% فقط من الضحايا يبلغون عن هذه الجرائم التي يصل معدلها إلى ألف جريمة يوميا. معهد أمن المعلومات أجرى دراسة مسحية بالتعاون مع مكتب التحقيقات الفيدرالية على 538 مؤسسة وشركة أمريكية فتبين أن 85% منها تعرضت لاختراقات إلكترونية، 70% منها جاءت عبر الإنترنت، و65% منها ألحقت خسائر مادية بالمؤسسة. ولم يتمكن سوى 35% من الشركات من حصر هذه الخسائر. لم يكن غريبا والأمر كذلك أن يطلب الرئيس الأمريكي السابق بيل كلنتون في يناير عام 2000م من الكونجرس تخصيص 2 مليار دولار لمكافحة جرائم الإنترنت.

(5)- **قدمت الولايات المتحدة الأمريكية**، مواطنا أمريكيا للمحاكمة الجنائية نتيجة قيامه بتقديم خدمة المقامرة عن طريق الانترنت، وإنشاء هذا الموقع في دولة انتيغوا وبربودا، وبيعه هذه الخدمة لمواطني الولايات المتحدة الأمريكية،

بالمخالفة لقانون الاتصالات السلكية لسنة 1961 (Wire Communication Act of 1961)، وهنا قضت المحكمة بحبسه 21 شهرا، ومنعت الموقع من الاستمرار. وبما أن اتفاقية الجاتس تنظم تبادل الخدمات عبر الحدود، وأمريكا ودولة انتيغوا وبربودا عضوان في الاتفاقية، فقد قدمت الأخيرة شكوى إلى لجنة فض المنازعات معتبرة حكم المحكمة الأمريكية مخالفا للاتفاقية وعائقا لحركة التجارة عبر الحدود.

ادعت أمريكا انها تمنع المقامرة عبر الانترنت في ولاياتها وفقا لقوانينها، وأن المقامرة عبر الانترنت تشكل مخالفة للآداب العامة، وأن المنع كان ضروريا ومبررا لحماية الأحداث من الوقوع في براثن المقامرين، ومنعا للجريمة المنظمة وغسيل الأموال، وبالتالي فإن لها الحق في منع مثل هذه الخدمات الالكترونية والتي تقدمها دولة انتيغوا وبربودا، وأن ذلك الحظر او المنع جاء متفقا مع اتفاقية الجاتس في المادة السابعة عشر فقرة (أ) والتي تمنح الدول الحق في وضع قيود على الخدمات التي تخالف الآداب العامة والنظام العام في 11 نوفمبر 2004 أصدرت اللجنة قرارها بأن الحظر والمنع الكامل للمقامرة عبر الانترنت والتي تقدم من دولة انتيغوا وبربودا لمواطني الولايات المتحدة الأمريكية غير مبرر وأن أمريكا تعسفت في استعمال حقها، لذلك فإن على أمريكا أن تلغي هذا المنع والحظر وفقا للاتفاقية ولتسهيل حركة التجارة والخدمات عبر الحدود.

وقد استندت لجنة فض المنازعات فى رفضها للأعذار المقدمة من أمريكا بناء على سببين رئيسين :

(1) على الرغم من الحظر المفروض بسبب الآداب أو الأخلاق العامة، كان ينبغي على أمريكا التفاوض مع انتيغوا وبربودا لمعرفة ما إذا كانت هناك بدائل أخرى أقل تقييدا لحرية التجارة بدلا من المنع الكامل، وعلى هذا الأساس فإن اللجنة لم تجد أن الحظر كان ضروريا لحماية الآداب العامة كما هو مطلوب في المادة السابعة عشر؛

(2) وجدت اللجنة أن أمريكا كانت تتعامل بطريقة فيها تمييز لصالح الموردين الأمريكيين، وأن تطبيقها للقانون كان غير محايد، حيث كانت تتم محاكمة الموردين الأجانب أكثر من الموردين الأمريكيين مما يعطي انطباعا أن أمريكا تفضل الموردين المحليين على الموردين الأجانب بدلا من تطبيق القانون المحلي الأمريكي على الجميع بدون محاباة أو تمييز.

هذه القضية تعتبر مهمة لسببين رئيسين:

أولا : أنها متعلقة بالمقامرة عن طريق الانترنت وما إذا كانت المقامرة تشكل مخالفة للآداب العامة من عدمه، أو أن هناك وسائل وطرقا أخرى للتقليل من آثاره بدلا من المنع الكامل أو أن المنع كان ضروريا لحماية الأخلاق العامة.

ثانيا : اتضح دور منظمة التجارة العالمية في الإشراف على حركة التجارة والوصول إلى القوانين المحلية للنظر في مدى ملاءمتها واتفاقها مع اتفاقيات التجارة الدولية، وتفسيرها للنصوص وسلطتها التقديرية في تقدير الحماية الضرورية لحفظ الأخلاق العامة في كل دولة.

لذلك، وبسبب عدم وضوح المقصود بالآداب العامة في قانون العقوبات الاتحادي، وفي قانون جرائم تقنية المعلومات، وما هو الممنوع وما هو المباح، وما يشكل جريمة، فإن منظمة التجارة العالمية قد تلعب دورا في التحديد وفي الإباحة قد لا يتفق مع غرض المشرع ورأي المحكمة الاتحادية العليا، وخاصة أن هناك أفعالا قد يختلف فيها وجهة النظر، وأن السلطة العامة لم تتخذ فيها أي إجراء عقابي يدل على المنع، مما قد يوهم في ذهن المنظمة ولجنة فض المنازعات إلى أن الأمر مباح غير مجرم، وأن منع دخول سلعة أو وقفها أو منع الحصول عليها ككتاب الكتروني فيه تقييد لحركة التجارة بالمخالفة لاتفاقيات التجارة الدولية، مما يؤثر على الثقافة

المحلية والعادات والتقاليد، ويجبر الطرف الآخر على قبول سلعة مما تخل بالآداب العامة وفقا لمفهومها في القوانين المحلية.

الجرائم السابقة ذات الطابع الاقتصادي أو السياسي تلقى اهتماما واسعا من المؤسسات المعنية بمكافحة جرائم الإنترنت، وهو اهتمام يفوق بمراحل الجرائم الأخلاقية على الإنترنت التي غدت من أكبر مسوقي تجارة الجنس في العالم. ومن سوء الحظ أن مكافحة الجرائم الجنسية على الإنترنت كثيرا ما تصطدم بعوائق تشريعية، ففى الولايات المتحدة الأمريكية، عطلت المحكمة العليا تطبيق قانون كان يستهدف حماية الأطفال من المواد الإباحية على الإنترنت رغم تزايد حالات استدراج الأطفال من خلال الشبكة والاعتداء الجنسي عليهم، القانون كان يفرض غرامة قدرها 5 ألف دولار على من ينشر مواد مؤذية للقصر على صفحات الإنترنت ويجعل تلك المواد في متناولهم بشكل يسير، لكن المحكمة اعتبرته مقيدا لضمانات حرية التعبير. الأمر نفسه حدث في هونج كونج حيث فشلت سلطات التشريع في وضع حد لترويج مواد إباحية للأطفال على شبكة الإنترنت ورفضت مشروع قانون يقضي بالحبس على كل من يثبت امتلاكه مواد إباحية تتعلق بالأطفال، وقال المشرعون: إنهم يخشون أن تتخذ السلطات ذلك القانون ذريعة لمزيد من إحكام قبضتها على الإنترنت. وعلى العكس من أمريكا وهونج كونج نجح المركز الاسترالي لمكافحة جرائم الإنترنت في توقيف وتفتيش 40 متهما بجرائم الاغتصاب والاستغلال الجنسي وتنظيم السياحة الجنسية وتوزيع أفلام دعارة باستخدام شبكة الإنترنت.

وقائع قرصنة أمام القضاء الأمريكى:

(1) ومن جرائم السرقة التى عرضت على القضاء الأمريكى نذكر أن أخصائي كمبيوتر روسى الجنسية ومقيم فى مدينة a st.peters burg

ويدعى Levin Vladimir هاجم نظم الكمبيوتر الخاص بـ city bank وذلك عبر واسطة asprint connection التى تربط روسيا بالولايات المتحدة ونجح فى الاستيلاء على مبلغ وقدره 10.000.000 عشرة مليون دولار أمريكى من حسابات البنك وقد تم ضبط Levin فى لندن عام 1995 وحكمت عليه إحدى المحاكم الأمريكية عام 1997 بالسجن لمدة ثلاثة أعوام.

وتشير حادثة سرقة city bank والتى وقعت خلال الهجوم على نظام الكمبيوتر الخاص بهذا البنك إلى تعاظم القدرات الإجرامية الخاصة بعصابات الجريمة المنظمة الروسية. ويشير التقرير الصادر بشأن الجريمة المنظمة الروسية [0(1)] إلى أن وزارة الداخلية الروسية (m.v.o) قد نجحت مؤخرا فى حل لغز إحدى جرائم الكمبيوتر الكبرى وذلك بالتعاون مع وحدة الخدمات الخاصة ببريطانيا وهولندا.

وتجدو الاشارة هنا إلى أن مجموعة كبيرة من موظفى البنوك الأجنبية قد زارت مقر city bank فى وقت سابق لوقوع الحادث بغرض دراسة نظام حماية الكمبيوتر الخاص بالبنك بصورة تفصيلية حتى يتمكنوا من تشغيل هذا النظام فى فروع البنك المنتشرة فى 96 دولة ومن بينها روسيا. ويعتقد أن المجرم قد اقتحم النظام من خلال وحدة الحماية الالكترونية ثم قام بسحب كميات كبيرة من المال من حسابات مجموعة كبيرة ومختلفة من العملاء وقام بتحويلها إلى حسابات تخص شركاته فى الجريمة تم فتحها مسبقا فى بنوك مختلفة خارج البلاد.

---

(1) تقدر وزارة الداخلية الروسية وهى الوكالة الروسية المسؤولة عن مكافحة عصابة الجريمة المنظمة الروسية أن ما بين 50% إلى 85% من البنوك الروسية تخضع لسيطرة تلك العصابات.

(2) عملية sundevil [1]:

حظيت عملية sundevil بشعبية واسعة فاقت مستواها من مختلف أنشطة مكافحة مخربي الكمبيوتر التى جرت عام 1990 فقد كانت حملة الضبطيات الواسعة التى استهدفت أجهزة الكمبيوتر المشتبه فيها فى سائر أرجاء الدولة والتى تمت فى 8 مايو 1990 حملة غير مسبوق بها من حيث النطاق والتغطية الإعلامية.

لقد كانت عملية sundevil اجراءا صارما استهدف فرض النظام على أولئك المخربين التقليديين الذين يعيشون فى " ظلال العالم الرقمى" سارقى بطاقات الائتمان ومسيئى استخدام أكواد التليفون،وكانت مجموعة sundevil أحد مجموعات مخربي الكمبيوتر والتى سميت العملية باسمها وهى أكبر المجموعات التى استهدفتها الحملة وأكثرها تنظيما. وقد استهدفت عملية sundevil بوصفها حملة على الاحتيال الالكتروني مجموعة منتقاة من جماعات المخربين تم اختيارها بعناية فائقة نتاجا لتحريات وتحقيقات مفصلة استمرت على مدار عامين كاملين.

ومرة أخرى كانت الأهداف هى نظم " لوحات النشر" وما من شك أن لوحات النشر قد تعد سندا قويا لعمليات الاحتيال المنظمة ودائما ما تحوى لوحات النشر السرية الخاصة بالمخربين - والمتداولة بينهم - مناقشات حية ومفصلة ومكثفة وصارخة لكافة أساليب وأنشطة انتهاك القانون والإخلال به وعلى الرغم من أن مناقشة تفصيلات القضايا الإجرامية ليست بالأمر غير المشروع، إلا أنه ليس بالامكان أن نعتبر الأشخاص الذين يتآمرون للانحلال بالقانون مجرد أندية أو صالونات فكر أو جماعات مستخدمين أو دعاة حرية

---

(1) أنظر فى ذلك :

The hacker Crackdown law and Disorder on the Electronic fron- tier by Bruce sterling p.159.1994.

رأى بل عادة ما توصفهم الشرطة وأجهزة الادعاء " بالعصابات أو المنظمات الفاسدة أو عصابة الجريمة المنظمة".

وما هو أكثر من ذلك، هو أن المعلومات والبيانات غير المشروعة التى تحويها لوحات النشر - الخارجة عن القانون- تتخطى فى عمقها مرحلة الحديث أو التآمر الجنائى المجرد فقد شهد حيز الممارسة فى ذلك العالم الرقمى السرى عمليات نشر الآلاف من أكواد التليفونات على لوحات النشر الخاصة بالمخربين تركت مشاعا لكل من تسول له نفسه إساءة استخدامها.

وقد حملت لوحات النشر الخفية المذكورة كذلك العديد من البرامج سهلة الاستخدام، التى تقوم باستعراض ومسح أكواد التليفونات وكذا المستخدمة فى الإغارة على نظم شركات بطاقات الائتمان، وإضافة إلى ذلك فطالما شهدت لوحات النشر المذكورة العديد من البرامج التى تعرضت لعمليات القرصنة وكلمات السر التي تعرضت للانتهاك ومخططات الاقتحام وأدلة العمل لراغب الاختراق وملفات التخريب والملفات الفاضحة وغيرها.

وتحظى لوحات النشر بجانب حيوى شيق يثير اهتمام المحقق المحترف إلا وهو أنها تعج بالأدلة الهامة فدائما ما نجد أن لوحات النشر توثق عمليات الاتجار فى البريد الالكتروني، كما تضم كافة الوقائع يتبجح المخترقون بنشرها تباهيا بأفعالهم غير المشروعة كما تعتبر أكواد التليفون وأرقام بطاقات الائتمان المسروقة ذاتها توثيقا الكترونيا وحقيقيا لأوجه النشاط الاجرامى. ويجب على المحقق- حال ضبطه لإحدى لوحات النشر الخاصة بالقراصنة أن يتعاملوا مع هذا الدليل بذات الاهتمام الذى يوجهه إلى التسجيلات التليفونية والمراسلات المعترضة التى يتحصل عليها فى القضايا العادية والمشكلة الحقيقية هنا هى أن قواعد الأدلة المتعلقة بتسجيلات التليفون ورسائل البريد المعترضة هى قواعد قديمة وصارمة ومفهومة جدا لرجال الشرطة والادعاء والمحاماة ، بينما لم تزل قواعد الأدلة المتعلقة بلوحات النشر قواعد جديدة ومعقدة وغير مفهومة لأحد على الإطلاق.

لقد كانت عملية sundevil أكبر حملة شهدها العالم حتى وقتنا الحالى على لوحات النشر الالكترونية غير المشروعة، فعلى مدار أيام 7،8،9 مايو 1990 تم ضبط حوالى 42 نظام كمبيوتر ومن بين الأجهزة التى ضبطها، وجد أن 25 جهازا كانت تدير فعليا لوحات نشر وقت الضبط.

لقد استطاعت الشرطة من خلال هذه الحملة الرائعة أن تسقط 25 لوحة نشر غير مشروعة فى ضربة واحدة، وتجدر الإشارة إلى أن الولايات المتحدة الأمريكية وحدها- تعج اليوم بما يقدر بـ300 ألف لوحة نشر الكترونية، فإذا ما افترضنا وجود لوحة نشر واحدة من بين كل مائة لوحة نشر عاملة تدار فى أغراض غير مشروعة سنجد أن 2975 لوحة نشر خارجة مازالت تعمل من على الأراضي الأمريكية ولم تمسها حملة sundevil الشهيرة. لقد ضبطت الحملة ما يقدر بثلث من نسبة1% فقط من اجمالى لوحات نشر الكمبيوتر فى أمريكا

لقد قام فريق متخصص من مكتب الخدمة السرية "بفونيكسش يدعمه أعضاء من مكتب المدعى العام بأريزونا- وهى منظمى عملية sundevil بإعداد قائمة فى عام 1990 تتضمن ما لا يقل عن 300 لوحة نشر ارتأوا أنها تستحق التفتيش والضبط، وقد كانت اللوحات الـ25 التى تم ضبطها فعليا من بين أكثر المواقع خطورة ووضوحا، وقد تم فحص كافة اللوحات التى تم ضبطها مسبقا- قبل عملية الضبط- سواء بمعرفة المرشدين أو بمعرفة عملاء مكتب الخدمة السرية أنفسهم، وقد أسهم هذا الفحص المسبق فى تحديد الاحتياجات الفعلية عند الإعداد للحملة، كما ساعد فى انتقاء الأشخاص المؤهلين لانجاز العمل.

وقد كان لعملية sundevil العديد من الدوافع التى نذكر منها فرصة تحقيق السبق الشرطى فى مجال جرائم الاحتيال الالكتروني والحصول على كم هائل من الأدلة الالكترونية لدراستها وفحصها وتقديمها للإدعاء.

وقد كانت عملية الضبط - فى صورتها المادية المجردة التى تمثلت فى إزالة الماكينات والمعدات- بمثابة أجراء هام خففت كثيرا من الضغط الذى طالما تعرضت له أجهزة الإنقاذ فى ذلك المجال.

لقد حرمت العملية الآلاف من لصوص بطاقات الائتمان والأطفال المتلاعبين بالأكواد من فرصة الالتقاء والتآمر والحصول على البيانات والمعلومات التى تساعدهم فى تحقيق مآربهم. وبضربة واحدة جعلت عملية sundevil كل هؤلاء الأفراد صم وعمى من الوجهة الرقمية الالكترونية.

وقد شنت أجهزة الانقاذ العديد من الهجمات المماثلة لعملية sundevil فى أحياء تقطنها أغلبية من البيض الذين ينتمون إلى الطبقة المتوسطة (الفئة المشتبه فيها) مثل: مونت ليبانون- بنسلفانيا، كلارك ليك يتشجان، وقد استهدف عدد قليل من هذه الهجمات مكاتب المشتبه فيهم بينما اتجهت الغالبية العظمى من الهجمات إلى المنازل حيث تم تفتيش غرف النوم والأبنية التى تعد بيئة مثالية لمخربى نظم الكمبيوتر.

ولم تكن عملية sundevil حملة اعتقالات - حيث لم يزد عدد المضبوطين فيها من الأفراد عن أربعة أشخاص- بل كانت حملة تفتيش وضبط. فدائما ما لا توجد أية اتهامات إلى مخربى نظم المعلومات حتى يتم تقييم الأدلة المتوافرة فى أجهزة الكمبيوتر الخاصة بهم والتى يتم ضبطها أثناء عمليات الضبط، وبالطبع فإن عملية تقييم أدلة الكمبيوتر تعد عملية مطولة للغاية فقد تستغرق أسابيع أو شهور أو أعوام، فإذا ما تم اعتقال أحد مخربى نظم المعلومات أثناء عملية الضبط، فإن ذلك يكون لأسباب أخرى بخلاف تورطه فى الجريمة الالكترونية (مثال: إحراز مخدرات أو حيازة سلاح غير مشروع).

ودائما ما يتعامل رجال الخدمة السرية مع مخربى نظم المعلومات على أنهم أناس أذكياء ومراوغين ولا يمكن التنبؤ بطبيعتهم أو سلوكياتهم فحقيقة

اختفاء المخرب وراء شاشة جهازه على مدى فترة طويلة من الوقت لا تحسن من صورته بأية حال من الأحوال أو تدعونا إلى الاعتقاد بأنه " مجرد طفل" وتجدر الإشارة إلى ضرورة تعامل الشرطة وأجهزة الإنقاذ مع مخرب نظم المعلومات وطوال الوقت بالقدر اللازم من الحرص.



المبحث الثالث

موقف التشريعات اللاتينية من جريمة سرقة المعلومات

أدى ربط الحاسبات الآلية بعضها بالبعض الآخر عن طريق شبكة المعلومات إلى سرعة انتقال المعلومات من جهة وإلى سهولة التطفل عليها واختلاسها من جهة أخرى عن طريق استخدام(المودم) modem [1]. حيث يسمح هذا الجهاز للمتطفلين من أي مسافة يتواجدون بها بالولوج فى الحاسبات الآلية المستهدفة ودون أي مساس مادى بحق ملكية الغير أو ترك أى أثر تدل على انتهاك المعلومات أو نسخها. ونظرا لجسامة هذا النوع من التعدى فقد حرص العديد من الدول على ارساء مبدأ لحماية وسلامة نظم المعلومات لديها وبغض النظر عن مبدأ حماية سرية البيانات المعالجة أو المتداولة.

وسوف نستعرض الحلول التشريعية التى استحدثت فى هذا المجال في بعض الدول أولا. ونعرض لذلك بشئ من التفصيل وفى القانون الفرنسى ثانيا.

أولا: الحلول التشريعية فى بعض الدول

فى السويد تنص المادة 21 من القانون رقم 289 الصادر فى 2 إبريل 1973 الخاص بالبيانات على أن " يعاقب.. كل من ولج بوسائل غير مشروعة إلى سجل مخصص لمعالجة البيانات آليا" أى أن القانون السويدي يعاقب على مجرد الولوج فقط.

(1) MODEM: عبارة عن أداة لترجمة تعليمات مكتوبة بلغة الحاسب الآلى إلى رموز رقمية أو العكس حيث يسمح للحاسبات الآلية أن تستقبل وتنقل المعلومات عن طريق وسيط لخط تليفونى.

وفى الدانمارك وطبقا للمادة 263 من قانون أول يوليه 1985 يعد من قبيل الجرائم فعل الولوج فى المعلومات أو البرامج المختزنة فى أجهزة المعالجة الالكترونية للمعلومات. وتستلتزم المشروعات الألمانية والنرويجية بقوانين أن يكون هناك انتهاك لتدابير الأمن لملاحقة مجرد الولوج فى نظم المعلومات.

ثانيا: التشريع الفرنسى

استحدث القانون الفرنسى الصادر فى 5 يناير 1988 بموجب المادة 2/462 عقوبات، جريمة الولوج غير المشروع فى نظم المعلومات والتى تنص على" يعاقب .... كل من ولج أو تواجد بطريق الغش فى كل أو جزء من نظام مبرمج للبيانات". وتشدد العقوبة إذا ما ترتب على ذلك إلغاء أو تعديل للبيانات التى يحتويها النظام أو إتلاف لوظيفة هذا النظام".

ويستهدف هذا النص فى المقام الأول حماية الولوج فى نظم المعلومات لا حماية حق الملكية ذاته وهو بذلك سد فراغا تشريعيا هائلا فى القانون الفرنسى، ومن جهة أخرى استجاب لرغبة ملاك الأنظمة المعلوماتية [1].

وتفترض هذه الجريمة توافر عنصرين أحدهما مادى والآخر معنوى.

أ-العنصر المادى:

يتحقق العنصر المادى لهذه الجريمة بمجرد شروع أى شخص- ليس له الحق – فى الدخول، أو تدخل بالفعل فى نظام مبرمج للبيانات.

ولكن هل يشترط لنشوء الجريمة أن يكون النظام محميا بواسطة جهاز أمن dispositif de securite! تمسك مجلس الشيوخ الفرنسى بهذا الشرط،

---

(1) راجع فى ذلك:

J.P.Buffelan,art.Prec.P.99.

وحجته فى ذلك جذب انتباه أصحاب الأنظمة إلى هذه النقطة الأساسية كى يدعموا أنظمتهم بأجهزة الأمن[1].

بينما رأت الجمعية الوطنية الفرنسية، أنه من غير المناسب التمسك بهذا الشرط، لأنه سوف يترتب عليه قصر الحماية الجنائية على الأنظمة المحمية بواسطة أجهزة الأمن ومن ثم يستبعد من مجال تطبيق النص أفعال الولوج التى ترتكب ضد الأنظمة المفتوحة للعامة [2] كالدليل الالكتروني أو الخدمات التى تقدم على رقم 36-15. وكتب لهذا الرأي الأخير النجاح، وتم التصويت على النص بدون حاجة إلى اقتضاء هذا الشرط.

ويتحقق التواجد غير المشروع، بمجرد علم الشخص بأنه تدخل بمحض الصدفة أو عن طريق الخطأ- وعلى نحو غير مشروع – فى نظام مبرمج للبيانات، ويستمر فى حال الاتصال به بدلا من الانفصال عنه فى الحال.

وهذه جريمة من جرائم الامتناع التى يصعب تقديم دليل أثبات فيها حيث يزعم المتهم دائما حال القبض عليه أنه كان على وشك الانفصال عن النظام المعتدى عليه[3] ويستوى أن يكون الولوج فى النظام المعتدى عليه كليا أو جزئيا حيث يستطيع المعتدى فى حالة التدخل المقترن بالغش، أن يدعى بسهولة بأن تحوله كان محدودا بجزء ضيق جدا من النظام، ولا يمكن التحقق من مثل هذا الإدعاء من الناحية العلمية[4].

---

(1) راجع فى ذلك:

J.Pradel,art prec,P.827, Lucas de leyssac, OP.CIT.P.21.

(2) انظر:

Rapport de r.Andre, Assemble Nationale,no.1078 "1987, 1988"P.5.

(3) راجع فى ذلك:

J.P.Buffelan,art. Prec,P.100.

(4) راجع فى ذلك:

F.Chamoux ,art prec ,H..Croze ,ART,PREC V. ROULET ,art prec.

ويقصد بالنظام المبرمج للبيانات:كل وحدة أو عدة وحدات للمعالجة و الذاكرة أو البرامج أو البيانات أو وحدات الإدخال والإخراج أو الموصلات التي تساعد فى الوصول إلى نتيجة محددة[1].

ويثور تساؤل، عما إذا كان الولوج غير المشروع يمكن أن يتحقق عن طريق ما يسمى بسرقة وقت الآلة أى استعمال مستخدم المنشأة أو الغير- على نحو غير مشروع- للحاسب الآلى فى الأغراض الشخصية.

يميل غالبية الفقه الفرنسى إلى بسط الحماية الجنائية الواردة بالمادة 2/462 عقوبات إلى سرقة وقت الآلة[2].

ب-لعنصر المعنوى:

يجب أن يتوافر لدى الفاعل قصد خلاص علاوة على القصد العام " أى اتيان الفعل غير المشروع عن علم وإرادة". والذى يتمثل فى نية الغش Fraudulcuscmcnt . ويقصد بالغش أن يباشر الفاعل سلوكه عن طريق الخديعة وبسوء نية وبغرض خداع الغير[3].

ويتمثل قصد الغش فى معرفة المتهم بأنه قد ولج أو تواجد فى نظام البيانات المبرمج ضد رغبة صاحب النظام وأيا كان الدافع إلى ذلك.

ولكن يثور التساؤل الآتي: هل يشكل النظام الآمنى للجهاز المعلوماتي عنصر من عناصر جريمة الولوج غير المشروع فى النظام المعلوماتي! هناك اتجاهان فى هذا الصدد.

---

(1) راجع فى ذلك: J.P.Buffelan,art prec P.100.

(2) انظر فى ذلك: J.Pradel ,art prec,P.823,h.CROZE ,ART PREC.

(3) أنظر فى ذلك: Lucas de Leyssac,OP.CIT.,P.20.

الاتجاه الأول:

ويرى[1] عدم ضرورة انتهاك نظام الأمن لكى تقوم الجريمة ويستند هذا الرأى إلى هل القانون، والأعمال التحضيرية له حيث تم رفض الرأى الذى كان يرى أنه من الضروري وضع تعريف لنظام المعالجة الآلية للبيانات - Sisteme traite ment automatise de donnees ويشترط وجود نظام أمان لذا وأنه طبقا لهذا الرأى فإن نظام الأمان لا يكون له إلا دورا واحدا هو إثبات سوء نية من قام بانتهاك النظام والدخول بطريقة غير مشروعة ولكن القصد الجنائي يمكن إثباته بطرق أخرى.

الاتجاه الثاني:

ويرى جانب آخر من الفقه ضرورة وجود نظام أمنى حيث أن القانون بجرم الاعتداء على نظم الأمن الخاصة بالنظم المعلوماتي ويستند هذا الرأي إلى ما يأتى:

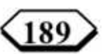
1- إن الاعتداء على النظام الأمنى يعتبر شرطا مفترضا فى جميع الجرائم المتعلقة بنظم المعلومات.

2- كما يستلزم كل من المنطق والعدل لهذا الشرط حيث أن القانون الجنائي لا ينبغى أن يقوم بحماية الأشخاص الذين لا يأخذون الاحتياط اللازم المتطلب من إنسان متوسط الذكاء. فوجود نظام حماية يمكن أن يكون التزاما مفروضا بنص القانون على كل من يقوم بإدارة نظام معلوماتى[2].

وفى الواقع أن قبول الاتجاه الأول من شأنه أن يؤدى إلى تجريم مجرد الدخول غير المشروع ولكن هل هذا التجريم ملائم من الناحية المنطقية والناحية القانونية.

(1) راجع فى ذلك:

(2) راجع فى ذلك: R.Gassin no.87 citant h. groze,OP.CIT ,no.10



الواقع أن الأسباب المتعلقة بضرورة وضع نظام أمنى فى نظم المعلومات تقتضى التفرقة بين أمرين:

الأمر الأول: حماية النظام بالمعنى الدقيق إذا وضعنا فى الاعتبار مدى أهمية حماية النظام بالمعنى الدقيق والمتطلب لتأمين النشاط الخاص بنظم المعلومات لوجدنا أن شركات التأمين تستلزم حد أدنى للأمن من جانب مستخدمي النظام حيث يمكن أن يطالبوا بالتعويض ومؤدى ذلك أن القانون الجنائى يوفر حماية واسعة بالنسبة لتلك الخاصة لشركات التأمين وهذا أمر منطقي.

ومن ناحية ثانية: فإن ضرورة تواجد النظام الأمني هو التزام قانوني وضروري منصوص عليه فى المادة 29 من القانون الصادر فى 6 يناير 1978 والخاص بنظم المعلومات والبطاقات والحريات[1].

حيث تستلزم هذه المادة كل شخص يعمل فى نطاق المعالجة الآلية للمعلومات الشخصية بضرورة اتخاذ الاحتياطات اللازمة لحفظ وحماية هذه المعلومات وخاصة بمنع تشويهها أو تعديلها أو الحصول عليها بواسطة أشخاص غير مرخص لهم بالاطلاع عليها[2].

---

(1) راجع فى ذلك:

LOI NO-87-17 du 6-01. 78 relative Informatique aux-. Fichiers ET aux libertes J.O du 7-01.78 ET. RE etificatgif au T.O.du 25.01.78.

(2) راجع فى ذلك:

Toute Personne ordonnatnt ou effectuant un traitement d informations nominatives s engage de ce Faitvis –a- VIS DES PER- sonnes concernees aprendre Toutes Precauions utiles afin de pre- sesverla Securite des information et notomment de empechet qu elles ne Soient deformees endommagees ou communiqués ades tiers non autorises.

article 29 de la loi NO.78-17.

di 6.01.78 Precitee.

وهكذا فإن الإخلال بهذا الالتزام الخاص بوضع نظام أمنى للجهاز والذى يقع على عاتق مستخدم النظام المعلوماتي للمعالجة الآلية لبيانات والمنصوص عليها فى المادة 29 تنطوى على جريمة جنائية معاقب عليها بالمادة 42 من قانون العقوبات الفرنسى والتى تنص على عقوبة السجن لمدة 5 سنوات.

موقف التشريعات الانجلوسكسونية من جريمة سرقة المعلومات:

سوف نتعرض فى هذه النقطة لبعض النماذج التشريعية للدول الأنجلو سكسونية وذلك على النحو التالى:

أولا: التشريع الانجليزى فى مجال جرائم إساءة استخدام النظم المعلوماتية

استحدث المشرع الانجليزى عام 1990 قانونا يعالج فيه إساءة استخدام نظم المعلومات وقد تم بموجب هذا التشريع تجريم عملية دخول أى فرد على البيانات المختزنة بالحاسب الآلى أو البرامج وكذلك عملية تعديلها بصورة غير مشروعة أو أى محاولة لفعل ذلك[1].

وقد نص القانون على ثلاثة جرائم محددة وهى [2]:

1- الدخول المتعمد غير المشروع:

Access is deliberate and unauthorized

(1) راجع فى ذلك:

Rapport de Mr. Andre au nom de la commission delois constitu- tiannelles de LA legistation et de l" administration generale de la republique sur la Proposition de m.Godfrain relative a la fraude informatique no. 744.P. 13. DOC. Ass .nat(1986/87) lly aura acces Frauduleux des lorsqu on cherchera a sintrodiure indumenta dans un systeme prcetege par un disposetif de Securite.

(2) **وقد أدرج القانون بعضا لتعريفات الآتية:**

- **البيانات:** هى تلك المعلومات الكائنة فى صيغة قابلة للمعالجة.
- **البيانات الشخصية:** هى البيانات المتعلقة بأفراد أحياء يمكن تحديد هويتهم.
- **الأشخاص المسند إليهم العمل فى مجال البيانات:** هم الأفراد المعينون بها.

2- الدخول غير المشروع والذى يتم بنية ارتكاب العديد من الجرائم.
3- قيام الفرد بأى فعل متعمد ينشأ عنه إجراء تعديل غير مشروع لمحتويات أجهزة الكمبيوتر.

ويلاحظ من صياغة هذا القانون ما يأتى:

أن المشرع الانجليزى يعاقب على التآمر والشروع والتحريض.

لا تلزم جهة الادعاء أن تقدم دليل يستفاد منه أن الأفعال المقترفة قد استهدفت بيانات أو برامج معينة.

لم يشترط القانون المشار إليه سلفا تواجد المتهم وقت ارتكاب الجريمة ولا بيانات الحاسب الآلى المستهدفة فى بريطانيا.

والتفسير الواسع لقانون السرقة theft act الانجليزى يشمل التلاعب فى البيانات من أجل الحصول على المنفعة المالية. فالمادة 15 من قانون السرقة الصادر سنة 1968 تنص على أنه " يعد مرتكبا لجريمة السرقة كل من حصل بطريق الغش أو بصفة غير مشروعة على مال يخص الغير بقصد حرمانه منه بصفة دائمة".

وكذلك تنص المادة الأولى من قانون السرقة الصادر سنة 1978على أنه "يعد مرتكبا لجريمة السرقة كل من حصل بطريق الغش وبصفة غير مشروعة على منفعة من الغير".

وتنص المادة 16 من نفس القانون على أنه " يعاقب كل من حصل بطريق غير مشروع وبأى وسيلة خداع سواء لنفسه أو للغير على منفعة مالية"[(1)].

---

(1) انظر فى ذلك:
M. BRAIT,la fraude informatiqu.. une .Approche de droit compare REV. dr.pen.cirm.p.290.

وعلى الرغم من أن ظاهر النصوص يوحى بإمكانية تطبيقها على سرقة المعلومات إلا أن القضاء الانجليزى تردد فى تطبيقها فى قضية Regina v.mortiz عام 1981 والتي تتعلق وقائعها بتلاعب أحد الأشخاص فى البيانات المعالجة الكترونيا بواسطة الحاسب الآلى والخاصة بسداد ضريبة TVA بهدف التهرب منها حيث اعتبرت المحكمة أن الغش الواقع على الآلة لا يعد من قبيل الاحتيال المعاقب عليها جنائيا وهذا ما دفع البرلمان الانجليزى إلى إجراء تعديل سنة 1983 يهدف إلى اعتبار خداع الآلة بنية ارتكاب غش مالى من قبيل الاحتيال المعاقب عليه جنائيا وهذا ما دفع البرلمان الانجليزى إلى أجراء تعديل سنة 1983 بهدف إلى اعتبار خداع الآلة بنية ارتكاب غش مالى من قبيل الاحتيال المعاقب عليه جنائيا[1] . وقد شمل قانون حماية البيانات الانجليزى الصادر سنة 1984 على المبادئ الآتية:

1- يجب الحصول على البيانات الشخصية – المخزنة لأغراض المعالجة- بأسلوب صحيح ولتحقيق أغراض مشروعة.
2- يجب حفظ تلك البيانات لأهداف محددة.
3- عدم جواز استخدام البيانات الشخصية إلا للغرض المحدد لها ولا يجوز الكشف عنها إلا بما يتفق مع ذلك الغرض المحدد لها.
4- لا يجب أن تتعدى البيانات الشخصية الغرض المحدد لها.
5- يجب توفير البيانات الشخصية للفرد المعنى بها مع التصحيح له بإجراء أى تعديلات لازمة لها.
6- يجب حفظ البيانات الشخصية بصورة آمنة تحميها من عمليات الدخول غير المشروع كما تحميها من الفقد.

(1) راجع في ذلك:

m.Briat,la fraud informatique, art prec.p.290.

الاستثناءات:

ويستثنى من هذا القانون البيانات الشخصية المختزنة المتعلقة بالرواتب، والمعاشات، وبيانات الحسابات، علاوة على الأسماء والعناوين المخصصة لأغراض توزيع المعلومات(مثال: إتحاد البريد).

وتستثنى كذلك البيانات الشخصية المخزونة المتعلقة بمجالات الأمن القومي أو منع الجريمة أو جمع الضرائب والرسوم.

وفى حالة جمع البيانات الشخصية لأغراض التحقيق أو الأغراض الإحصائية فقط، أو حفظها كنسخة إضافية مجردة، لا يحق للأشخاص المسند إليهم العمل فى مجال البيانات الاطلاع عليها وبالرغم من وجوب تأمين البيانات الشخصية إلا أنه من الممكن أن يتم الكشف عنها لوكلاء أصحابها(مثال: المحامى أو المحاسب) أو لأحد الأشخاص العاملين لدى مستخدمى البيانات أو لأى شخص آخر فى حالة وجود حاجة ملحة لمنع وقوع إصابة أو أضرار بالصحة.

- أساليب حماية البيانات: وتتعدد هذه الأساليب طبقا للقانون الانجليزي على النحو التالى:

1- الحماية عن طريق كلمة السر (كلمة المرور):

عادة ما يتم تخزين أسماء المستخدمين وكلمات المرور فى جداول، ويحفظ هذا الجدول بشكل دائم على ملف موجود على اسطوانة. وغالبا ما تحفظ جداول كلمات المرور جنبا إلى جنب مع جداول التفويض التى تحوى حقوق المستخدم فيما يتعلق بالملفات الأخرى، ويجب ألا تكون جداول كلمات المرور مشفرة على نحو " لا يمكن تعديله" وذلك لتجنب إمكانية الاطلاع على محتوياتها.

2- تشفير البيانات:

تقوم عملية التشفير على تحويل الرسالة من نص واضح إلى نص مشفر، ويتم إرسال الرسالة المشفرة عبر قناة اتصال، حيث يقوم الحاسب المتلقي بفك شفرة الرسالة.

التدابير الأمنية الأخرى:

بخلاف كلمة المرور، يمكن التعرف على المستخدم المصرح له وذلك عن طريق:

- التعرف على بصمة العين.
- التعرف على بصمات الأصابع.
- التعرف على الصوت.
- التعرف على الوجه:

ثانيا : التشريع الاسترالى:

تبنت غالبية الولايات فى استراليا تفسيرا واسعا لمفهوم السرقة مستوحى من القانون الانجليزى. ويبدو ذلك واضحا فى قضية حيث أدانت إحدى المحاكم الاسترالية شخصا بجريمة السرقة لاحتياله على مدير إحدى البنوك فى سيدنى حيث أنه تلاعب فى برامج الحاسب الآلى كى تبدو الاعتمادات المالية فى صالحه[1].

ويختص قسم جرائم الكمبيوتر التابع للبوليس الفيدرالى الاسترالى والذى تكون عام 1989 بمهمتين رئيسيتين - المهمة الأولى هى البحث والتقصى وجمع المعلومات الاستخباراتية عن جرائم محددة من جرائم الكمبيوتر بينما المهمة الثانية هى توفير الدعم الفنى لوحدات البحث والتحقيق السرى

(1) راجع فى ذلك:

m. Briat ,la fraude informatique ,art prec .p.291.

المنهمكة فى التحقيق فى الجرائم المتصلة بالكمبيوتر أو التى تعتمد عليه فى ارتكابها.

والتشريع الذى يحدد مسئولية البوليس الفيدرالى الاسترالى بشأن جرائم الكمبيوتر المحددة يوجد فى قانون العقوبات لدول بالكومنولث والصادر عام 1914 (الجزء6أ) والذى يشمل الأقسام من 76 أ إلى 76ف. هذه الأقسام المتعلقة بالأفعال الإجرامية تشمل قائمة بالظروف والملابسات التى تشكل فعلا إجراميا ودرجة العقوبة المحتملة المرتبطة بهذه الأفعال. وقد تم وضع هذا التشريع فى يوليو 1989 وتم تعديله فى 1991. ولدى البوليس الفيدرالى الاسترالى الحق السيادى لتطبيق هذا التشريع فى أحد موقفين:

الموقف الأول: كان الكومنولث يتمتع بالسلطة والحق فى تطبيق هذا التشريع حينما كان الفعل الإجرامي موجها نحو الكمبيوتر التابع للكومنولث، أو أحد أجهزة الكمبيوتر التى تحتوى على بيانات أو معطيات لصالح الكومنولث. والإشارة إلى البيانات أو المعطيات التى تم تخزينها فى الكمبيوتر لصالح الكومنولث تشمل الوضع حينما يتم تخزين هذه البيانات والمعلومات بناء على توجيه أو طلب من الكومنولث.

الموقف الثانى: فيمكن تطبيق هذا التشريع حينما يكون الفعل الاجرامى موجها ضد أى كمبيوتر بواسطة أى تسهيل يتم تشغيله أو توفيره بمعرفة الكومنولث أو بمعرفة أى طرف وسيط، وتعريف الوسيط أمر واسع النطاق وهو يشمل كافة المنظمات، سواء الخاصة أو الحكومية، التى تقوم بتزويد هذه الخدمة بموجب ترخيص ممنوح طبقا لقانون الاتصالات عن بعد الصادر عام 1991.

وبصفة أساسية نبين فيما يلى الفئات الأربعة للأفعال الاجرامية الواردة فى هذا التشريع:

الفئة الأولى: هى الأفعال الإجرامية الخاصة بالكمبيوتر التى تتعلق بالوصول غير القانونى للكمبيوتر والحد الأقصى للعقوبة عن هذا الفعل ابن حزم الحبس لمدة 6 أشهر.

الفئة الثانية: من الأفعال الإجرامية الخاصة بالكمبيوتر تتعلق بالوصول غير القانوني لأحد أجهزة الكمبيوتر بقصد خداع شخص معين والتدليس عليه والحد الأقصى للعقوبة عن هذا الفعل هو الحبس لمدة سنتين.

الفئة الثالثة: من الأفعال الإجرامية تتعلق بالوصول غير القانوني إلى أجهزة الكمبيوتر والاطلاع على أنواع معينة من البيانات والمعلومات.

الفئة الرابعة: من هذه الأفعال الإجرامية فهى تطابق نوعين معينين من الآثار المترتبة على نظام الكمبيوتر التى ترقى لمستوى الفعل الإجرامي حينما يتم التسبب فى هذه النتائج عن عمد.

ثالثا: التشريع الكندى

استحدث قانون العقوبات الكندى[1] المادة *301* فقرة *2* والتى تنص على:

أ- كل من حصل بطريق الغش وبدون وجه حق مباشرة أو بطريق غير مباشر على خدمات من حاسب آلى.

ب- كل من ولج بنية الغش، بواسطة جهاز الكتروني أو صوتى أو آلى مباشرة أو بطريق غير مباشر فى حاسب آلى.

جـ- كل من استعمل حاسب آلى مباشرة أو بطريق غير مباشر بغرض ارتكاب جريمة منصوص عليها فى الفقرة أ،ب أو جريمة منصوص عليها فى المادة 387 خاصة ببيانات أو حاسب آلى يعد مرتكبا لفعل إجرامى ويعاقب بالحبس لمدة عشر سنوات.

وتنص المادة **387** يعد مرتكبا لعمل آثم كل من باشر عمدا:

أ- إتلاف أو تعديل البيانات.

ب- سرقة البيانات أو جعلها غير صالحة أو عديمة الفائدة.

جـ- منع أو إعاقة الاستخدام المشروع للبيانات.

---

(1) راجع فى ذلك:

Vivant et le stanc, lamy informatique no.2489.

د- منع أو إعاقة شخص فى استخدام حقه المشروع للبيانات أو رفض ولوج شخص له الحق فى البيانات.

ثالثا: التشريع الأمريكى

يطبق فى الولايات المتحدة الأمريكية القوانين الخاصة بالغش فى مجال البنوك والبريد والتلغراف والاتفاق ألأجرامي لأغراض ارتكاب الغش على جرائم سرقة المعلومات. بل أن بعض الولايات الفيدرالية أصدرت قوانين بموجبها أعطت مفهوما واسعا للمال بحيث يشمل " كل شى ينطوى على قيمة" ويندرج تحت هذا التعريف الأموال المعنوية والبيانات المعالجة وتعاقب هذه القوانين على الاستخدام غير المسموح به بغرض ارتكاب أفعال الغش أو للاستيلاء على المال[1] وعلى المستوى الفيدرالى صدر قانون

(1) استحدثت الولايات الأمريكية (مثل أريزونا وكاليفورنيا وكولورادو وديلادار وفلوريدا وجورجيا والبنوى وميتشجان وميسورى ومونتانا وأوتارا ونيومكسكو...)العديد من القوانين الجنائية التى تعاقب على الاستخدام غير المسموح به للحاسب الآلي بغرض الاحتيال أو الحصول على مال والمجال هنا ليس متسعا لفحص جميعها، ولذا نكتفي بإيراد ملاحظتين عليها:

أولاهما:أن آليات التجريم فى هذه القوانين على درجة كبيرة من الاختلاف ويبدو ذلك من زاويتين:

(أ) أن جميع هذه القوانين إذا كانت تتمسك بضرورة توافر الغش أو سوء النية فى الأفعال المعاقب عليها إلا أن صيغتها فى هذا الشأن جاءت غير مطابقة وعلى سبيل المثال فقانون كاليفورنيا ينص على أن " يعاقب كل شخص ولج عن عمد أو سوء نية...." مادة 502 من قانون عقوبات كاليفورنيا الصادر سنة 1979 والمعدل سنة 1982 " وقانون ديلادار" ينصان على" كل من .... وكان ذلك عن تبصر ـ أو تروى مباشر أو بطريق غير مباشر" مادة 558 والمعدلة فى سنة 1982، وقانون فلوريدا ينص على " كل من باشر.... عن تروى وعلم وبدون إذن......" وقانون 1978 سوقانون بنسلفانيا" ينص على" كل من .... عمدا وبدون إذا " قانون سنة 1983".

(ب) أن بعض هذه القوانين مال إلى تقنين وبشكل مختصر الأفعال المجرمة مقتديا فى

الولوج المصطنع فى الحاسب الآلى فى أكتوبر سنة 1984[1]

ذلك بالنموذج الفيدرالى ومنها قانون كاليفورنيا والذى يعاقب " كل من ولج عمدا فى نظام أو شبكة معلوماتية بفرض محاولة أو تنفيذ أى مؤامرة أو حيلة بغرض الحصول على نقود أو خدمات " قانون العقوبات مادة 502/ب" ويجرم هذا القانون أيضا " كل من ولج وبسوء نية فى نظام شبكة معلوماتية بغرض الحصول على معلومات غير مسموح بها تتعلق بسمعة الغير أو كل من أدخل معلومات مصطنعة بغرض تحسين أو اساءة سمعة الغير ويعاقب أخيرا كل شخص ولج بسوء نية أتلف أو محا أو أضر بأى نظام معلوماتي أو شبكة معلوماتية أو كيان منطقى أو بيانات وعلى النقيض تنبت بعض القوانين الأخرى المنهج التحليلى ومنها على سبيل المثال قانون فلوريدا والذى احتوى على ثلاث مجموعات أساسية إحداهما: مخصصة للجرائم التى تقع على البيانات الموجودة بالبرامج والثانية: خاصة بالجرائم التى تقع على المعدات والتجهيزات المعلوماتية والثالثة : خاصة بجرائم المستخدمين لنظم المعلومات، ولكل مجموعة منها قواعدها الداخلية الخاصة بها وثانيهما: تتعلق بالمنهج الانجلو سكسونى فى التعاريف القانونية حيث يلاحظ أن هذه التعاريف ليس لها أى قيمة خارج الولايات المتحدة بل وأيضا خارج الولاية التى تنص عليها، وفضلا عن ذلك فليس لها أى قيمة خارج النص الذى يحتويها حيث أنها تعطى من أجل احتياجات النص.

راجع فى ذلك:

Vivant et le stanc, lamy droit de informatique ,no.2487.

(1) بدأت - أنفينا سيكوريتى كورب - فى بادئ الأمر وكأنها شركة انترنت نموذجية، بمكاتبها وحاسباتها وموظفيها ونظامها الأمنى الحاسوبي ولم يكن ينقصها سوى الزبائن. لكن تبين الآن أن تلك الشركة التى بدت مشروعا فاشلا للوهلة الأولى كانت شركة وهمية أنشاها مكتب التحقيقات الفيدرالية الأمريكى اف بى أى للايقاع بشابين روسيين متهمين باختراق كمبوترات شركات انترنت أمريكية واختلاس معلومات حساسة فى محاولة لابتزاز المال وتقول السلطات إن اليكسى ايفانوف 21 عاما وفاسيلى جورشكوف 25 عاما وكليهما من مدنية شليابنسك الروسية قد ابتلعا الطعم ووقعا فى فخ الإف بى أى. وفى حين رفض مكتب التحقيقات الفيدرالية

counterfeit access device and computer Fraud and abuse act والذى ولج عمدا فى حاسب آلى بدون إذن أو كان مسموحا بالولوج منه، واستغل الفرصة التى سنحت له عن طريق هذا الولوج لأغراض لم يشملها الإذن، وقام عمدا عن طريق هذه الوسيلة باستعمال أو تعديل أو إتلاف أو إفشاء معلومات مختزنة فى الحاسب متى كان هذا الأخير يعمل باسم ولصالح الحكومة الأمريكية، وطالما أثرت هذه الأفعال على أداء وظيفته. ويمكن لهذا النص وبطريق غير مباشر وبشروط معينة أن يشمل النصب الذى يرتكب عن طريق الحاسب الآلي، ولكن وزارة العدل الأمريكية قدمت فى أغسطس سنة 1984[1]

=

الإدلاء بأية تعليقات فإن وثائق قضائية كشف عنها النقاب مؤخرا تبدو وكأنها رواية جاسوسية يروى فيها عملاء الاف بى آي كيف تمكنوا من الإيقاع باللصين عن طريق انشاء شركة زائفة ودعوة ايفانوف وجوشكوف لمحاولة اختراق أنظمتها الحاسوبية المحصنة، وبعد أن نجح القرصانان الروسيان فى اختراق الأنظمة عن بعد وجه موظفوا شركة أنفيتا دعوة لهما للقدوم إلى سياتل فى الولايات المتحدة لمناقشة

ابرام عقد شراكة واستعراض كامل امكانياتهما فى مجا ل التسلل إلى أجهزة الكمبوتر عبر الانترنت، وبينا كان الشابان يستعرضان مهاراتهما فى الشراكة الوهمية استخدم الاف بى آي تقنية تصنت حاسوبية تبسط نشاطها عبر الانترنت وتخترق النظام الحاسوبي الخاص بالمتهمين فى روسيا.

ويقول خبراء أمن الانترنت أن القضية تعرض لمدى تطور مقدرات مكافحة جرائم الانترنت لدى مكتب التحقيقات الفيدرالية لكن الدفاع يشير الاستفهام حول مشروعية استخدام هذه الأساليب.

راجع فى ذلك: جريدة البيان - دبي - الإمارات العربية المتحدة، العدد 7633 تاريخ 12 مايو 2001.

(1) صدر فى الولايات المتحدة الأمريكية القانون الفيدرالى بشأن الغش والعبث المعلوماتى computer fraud & abuse act فى عام 1984 وأدخل عليه تعديلات كان آخرها عام 1996. ويواجه هذا القانون عدة أفعال تتصل بالدخول غير المشروع أو الحصول متجاوزا التصريح على معلومات تتعلق بالدفاع الوطنى أو العلاقات

=

مشروعا بقانون يستهدف مباشرة حالة الغش المعلوماتى والذى يعاقب " كل من رتب أو صمم خطة ما أو حيلة بغرض ارتكاب غش أو الاستيلاء على مبلغ من النقود أو مال لا يخصه وولج أو حاول الولوج فى حاسب آلى بغرض تنفيذ أو محاولة تنفيذ هذه الخطة أو الحيلة أو لارتكاب أو محاولة ارتكاب مثل هذا النصب أو هذه السرقة أو الاختلاس....." ومصطلح المال property وفقا لهذا المشروع بقانون يشمل " كل الوسائل المالية والمعلومات التى تحتوى على بيانات معالجة والمكونات الالكترونية والكيانات المنطقية وبرامج الحاسب الآلي سواء بلغة الآلة أو بلغة مقروءة للإنسان وكل قيمة أخرى ذات طابع مادى أو معنوى"[1].

وقد خول الكونجرس الأمريكى[2] قطاع الخدمة السرية سلطة التحقيق فى عمليات الاحتيال التى تتم عبر الشبكات والتى تعرف باسم " عمليات التحايل على وسائل الدخول للمعلومات. وذلك بموجب البند رقم 18 من قانون الولايات المتحدة الأمريكية القسم 1029 ويضم القسم المذكور تعريفا عاما لمصطلح وسائل الدخول للمعلومات وهو: «أية بطاقة أو لوحة أو رقم

=

الخارجية لا يجوز الكشف عنها. ويعاقب أيضا على نقل مكونات لبرامج أو معلومات دون موافقة من صاحب الشأن فى حالة ما إذا ترتب على هذا النقل خسائر لشخص أو أكثر، ويواجه القانون أيضا مشكلة غش كلمات المرور بما يمكن مرتكبه من الدخول على نظام للكمبيوتر إذا كان من شأنه الإضرار بالتجارة بين الولايات بالتجارة الخارجية. راجع فى ذلك: د. طارق سرور، سابق الإشارة إليه ،ص53.

(1) راجع فى ذلك:

Mendes"m.w" la legislation penale en matiere d ordinateurs et les measures de securite aux ETATS- Unis , Droit de informatique mumero special 1985.p.41.

(2) انظر فى ذلك:

The Hacher crackdown law and Disorder on the Electronic fron – tier by Bruce sterling p.0172,1994.

كودى أو رقم حساب أو أية وسيلة أخرى من وسائل الدخول على الحسابات بغرض التحصل على أموال أو بضائع أو خدمات أو أى شئ آخر ذو قيمة يمكن استخدامه كوسيلة من وسائل بدء نقل الأموال».

ومن هنا نرى أن المصطلح يمكن أن يتسع بحيث يشمل بطاقات الائتمان وأرقام حساباتها وكذا بطاقات الشحن الهاتفية وأكواد الدخول على التليفونات ويلاحظ على نص القسم 1029 أنه وقد منح قطاع الخدمة السرية سلطة ومباشرة فى مواجهة ذلك" العالم الرقمى الخفى" دون أن يشير من قريب أو بعيد لكلمة كمبيوتر.

وتتوافر العديد من وسائل الاحتيال القياسية التى تعرف بإسم " الصناديق الزرقاء" وتستخدم لسرقة الخدمات التليفونية من أجهزة المفتاح الآلى القديم وبالطبع فإن مثل هذه السرقات تعد من بين عمليات " الاحتيال باستخدام وسائل الدخول للمعلومات" وبفضل أحكام القسم 1029، لم يقتصر الأمر على الإقرار بعدم مشروعية عمليات " استخدام وسائل دخول" مزيفة بل أمتد ليشمل عمليات تخليقها كذلك فقد أدرجت عمليات «الإنتاج» و«التصميم» و «النسخ» و «الجمع» الخاصة «بالصناديق الزرقاء» ضمن الجرائم الفيدرالية.

وتعد ماكينات الصرف الآلية - التى انتشرت فى سائر أرجاء الولايات المتحدة الأمريكية خلال حقبة الثمانينات- من بين «وسائل الدخول للمعلومات» وتعتبر أية محاولة للمسها بالضغط على لوحة مفاتيحها، أو التلاعب فى البطاقات البنكية البلاستيكية بمثابة فعل يندرج تحت طائلة العقوبات المدرجة بالتقسم 1029.

ويتسم القسم 1029 بالمرونة والوضوح فإذا ما افترضنا عثور أحد الأشخاص على كلمة المرور الخاصة بإحدى أجهزة الكمبيوتر داخل صندوق قمامة شخص آخر!! فإن كلمة المرور هذه تعتبر " كود" أو " وسيلة دخول على الحساب". وكذا إذا ما افترضنا أن أحد الأشخاص قد تمكن من الدخول

على إحدى أجهزة الكمبيوتر وقام بنسخ بعض البرامج المخزونة عليه لحسابه الخاص، فهو بذلك قد حصل على " خدمة" " خدمة جهاز كمبيوتر" وكذا "شى ذو قيمة" (البرنامج المنسوخ) دون وجه حق. وأخيرا إذا ما افترضنا أن أحد الأشخاص قد قام بإطلاع مجموعة من أصدقائه على كلمة المرور التى عثر عليها أو سرقها، وتركهم أو شجعهم على استخدامها فهو بذلك " يتاجر فى وسائل الدخول غير المشروعة".

ويشتمل القسم **1029** على بندين:

أولهما: ضرورة " تأثير الجرم على التجارة الداخلية أو الخارجية للدولة كى تقع تحت طائلة ونطاق الاختصاص الفيدرالى.

وثانيهما: فيتعلق بحجم المال، فهناك قاعدة تقضى بعدم قيام المسئولين الفيدراليين بتتبع المجرمين المتورطين فى جمع مبالغ بسيطة من المال. حيث أن الجرائم الفيدرالية يجب أن تتسم بالخطورة ويحدد القسم 1029 الحد الأدنى للخسارة المالية التى تقع تحت طائلة القانون الفيدرالى بمبلغ ألف دولار أمريكى.

وقد منح القسم 1030 الخاص بـ" الاحتيال والأنشطة ذات الصلة المرتبطة بالكمبيوتر" منح قطاع الخدمة السرية السلطة القانونية المباشرة على كافة الأعمال المتصلة باختراق الكمبيوتر.



المبحث الرابع

آليات مكافحة الجريمة الإلكترونية فى الدول الغربية

اقتناعا بالحاجة إلى تحقيق سياسة جنائية مشتركة رأت الدول الأعضاء في المجلس الأوروبي وبعد التوصيات التي تقدمت بها اللجنة الأوروبية حول مشكلات الجريمة في مجال جرائم الكمبيوتر تم توقيع الاتفاقية الأوروبية بشأن جرائم الكمبيوتر بتاريخ 23/11/ 2001م بغرض حماية المجتمع الأوروبي من جرائم الكمبيوتر وذلك من خلال التقريب بين التشريعات القانونية الجزائية ولتمكين وسائل التحقيق الفعالة فيما يتعلق بهذه الجرائم، وفتح الباب أمام أكبر عدد ممكن من الدول لكي تصبح أطرافا في الاتفاقية لحاجة المجتمع إلى نظام سريع وفعال للتعاون الدولي ،والذي يأخذ بعين الاعتبار المتطلبات المحددة لمكافحة جرائم الكمبيوتر.

وتتكون هذه الاتفاقية من **48** مادة مقسمة إلى أربعة فصول على النحو التالي:

الفصل الأول يتضمن تعريفا للمصطلحات الواردة في الاتفاقية ومنها تعريف بنظام الحاسوب والذي بعني أي جهاز أو مجموعة من الأجزاء المتصلة فيما بينها، أو أي أجهزة أخرى ذات علاقة، والتي يقوم واحد أو أكثر منها، بحسب برنامج ما بالمعالجة الأوتوماتيكية للبيانات ، كما بين هذا الفصل ما المقصود ببيانات الحاسوب وهو أي عرض أو تمثيل للحقائق أو المعلومات أو الأفكار بشكل ملائم لمعالجتها في نظام الحاسوب ،بما في ذلك أي برنامج ملائم يؤدي لقيام نظام الحاسوب بالعمل وأداء وظيفة ما، وكذلك عرف مزود الخدمة بأي جهة عامة أو خاصة توفر لمستخدمي خدماتها القدرة على الاتصال بطريق نظام الحاسوب أو أي جهة أخرى تعالج أو تخزن بيانات الحاسوب بالنيابة عن جهة الاتصال أو مستخدمي ذلك الخدمة، كما عرف مرور البيانات بمعني أي بيانات حاسوب متعلقة بأي اتصال بطريق نظام الحاسوب، ينشئها نظام الحاسوب بشكل جزء من سلسة اتصال،

تشير إلى منشأ الاتصال أو اتجاهه أو طريقه أو وقته أو بياناته أو حجمه أو مدته أو نوع الخدمة أساسا.

أما الفصل الثاني من هذه الاتفاقية فيقع تحت عنوان الإجراءات الواجب اتخاذها على المستوى والوطني والمتمثلة في أن تتبنى التشريعات الجنائية الوطنية (قانون العقوبات العام) للدول الأعضاء في الاتفاقية جرائم ضد سرية وسلامة وتوفر بيانات وأنظمة الحاسوب ، كالدخول غير المشروع والتدخل غير المشروع وتشويش البيانات وتشويش النظام وإساءة استخدام الأجهزة والتزييف المرتبط بالحاسوب والاحتيال والجرائم المرتبطة بالصور الإباحية للأطفال والجرائم المرتبطة بالتعدي على حقوق الطبع والحقوق الأخرى ذات العلاقة والمسؤولية والعقوبات الإضافية. ومن جانب آخر أن تتبنى الدول الأعضاء في قانون الإجراءات الجنائية تحديد السلطات والإجراءات الواردة في الاتفاقية بغرض إجراء التحقيقات والإجراءات الجنائية المحددة. وكذلك تبيان الشروط واحتياطات الأمان المتمثلة في توفير الحماية الكافية للحقوق وحريات الإنسان، بما في ذلك الحقوق الناشئة عن أي التزامات أخذتها الدول الأعضاء على عاتقها بموجب اتفاقية المجلس الأوروبي لعام 1950م، حول حماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للحقوق المدنية والسياسية لعام 1966م وأي أدوات دولية حول حقوق الإنسان.

وكذلك أكدت الاتفاقية على ضرورة تحديد الاختصاص بشأن أي جريمة وردت وفقا لأحكام هذه الاتفاقية، عندما ترتكب الجريمة على إقليم الدولة الطرف في الاتفاقية أو على متن سفينة ترفع علمها أو على متن طائرة مسجلة بموجب قوانينها أو من قبل أي من مواطنيها، إذا كانت الجريمة معاقب عليها بموجب قانونها الجنائي أو إذا ارتكبت الجريمة خارج الاختصاص الإقليمي لأي دولة .

كما حددت الاتفاقية في الفصل الثالث منها المبادئ العامة المتعلقة بالتعاون الدولي والمتمثل في تطبيق الأدوات الدولية ذات العلاقة حول التعاون الدولي في الشؤون الجنائية والإجراءات المتفق عليها على أساس التشريع الموحد أو المتبادل والقوانين المحلية ،إلى أقصى مدى ممكن لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المرتبطة بأنظمة وبيانات الحاسوب أو لجمع الأدلة بشكلها الإلكتروني في جريمة جنائية إضافة إلى ذلك الإشارة إلى المبادئ المتعلقة بالتسليم في الجرائم الجنائية الواردة في الاتفاقية بشرط أن تكون معاقب عليها بموجب قوانين كلا الطرفين المعنيين بسلب الحرية لمدة أقصاها سنة واحدة على الأقل أو بعقوبة أشد.

وكذلك الجرائم الجنائية التي يجب أن يتم اعتبارها قابلة للتسليم ،أو إذا كان هناك طرف يجعل التسليم مشروطا بودود اتفاقية تسليم، ثم تلقى طلب تسليم من طرف آخر ليس لديه اتفاقية تسليم معه،فيجوز له أن يعتبر هذه الاتفاقية أساسا قانونيا للتسليم فيما يتعلق بأي جريمة جنائية مشارا إليها في الاتفاقية.

كما وضعت الاتفاقية مجموعة من المبادئ العامة المتعلقة بالمساعدة المتبادلة لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المرتبطة بأنظمة وبيانات الحاسوب، أو لجمع الأدلة بشكلها الإلكتروني في أي جريمة جنائية، كما بينت الإجراءات المتعلقة بطلبات المساعدة المتبادلة في غياب الاتفاقيات الدولية القابلة للتطبيق.كما استخدمت الاتفاقية مصطلح الشبكة بمعنى أن على كل طرف أن يعين نقطة اتصال متاحة بواقع (24) ساعة في اليوم سبعة أيام في الأسبوع، لضمان توفير المساعدة الفورية لأغراض التحقيقات أو الإجراءات في الجرائم الجنائية المرتبطة بأنظمة الحاسوب والبيانات، أو لجمع الأدلة بشكلها الإلكتروني في جريمة جنائية،

مثل هذه المساعدة ستشمل، إذا سمح بذلك القانون المحلي والممارسة، تسهيل أو القيام مباشرة بما يلي:

أ- توفير المساعدة الفنية.

ب- حفظ البيانات وفقا لما نصت عليه الاتفاقية.

ج- جمع الأدلة وإعطاء المعلومات القانونية، وتحديد المشتبه بهم.

واختتمت الاتفاقية الفصل الرابع بأحكام نهائية والتي تضمن العديد من الأحكام والتي من ضمنها إجراء مشاورات بين الأطراف بشكل دوري من اجل تسهيل الأمور التالية:

أ- الاستخدام والتطبيق الفعال لهذه الاتفاقية بما في ذلك تحديد أي مشكلات تعترض سبيلها ، وكذلك تأثيرات أي تصريح أو تحفظ تم وفقا لها.

ب- تبادل المعلومات حول التطورات القانونية أو التكنولوجية الهامة أو حول السياسة المتعلقة بجرائم الحاسوب وجمع الأدلة بشكلها الإلكتروني.

ج- دراسة إمكانية استكمال أو تعديل الاتفاقية.

بهذا نرى أن هذه الاتفاقية تعد أول وثيقة قانونية دولية (أوروبية) تعتمد تدابير وأحكام حول جرائم الحاسوب والتي جسدت القلق البالغ الذي يساور الدول الأطراف، إزاء جسامة وخطورة جرائم الحاسوب، ومؤمنة بأن العمل الفعال ضد جرائم الحاسوب يتطلب تعاونا دوليا متزايدا وسريعا وفعالا في الأمور الجنائية وكذلك الحاجة لحماية المصالح المشروعة في استخدام وتطوير تكنولوجيا المعلومات.



الفصل الخامس
جرائم الإنترنت فى التشريعات المقارنة

يركز هذا الفصل على تبيان موقع جرائم الانترنت -على وجه الخصوص- فى التشريعات المقارنة من خلال سبعة مباحث ركز الأول منها على جريمة العدوان على الإئتمان الرقمى فيما تناول المبحث الثانى جريمة الاحتكار والاحتكار المضاد وتناول المبحث الثالث جرائم الأخلاق، وتحدث المبحث الرابع عن جريمة الترويج السمعى-المرئى الفاضح، واختص المبحث الخامس بجريمة البث العلنى وتشمل النشر والسب والقذف والتشهير والمراسلة وجاء المبحث السادس متناولا جريمة المطاردة والإزعاج.



المبحث الأول
جريمة العدوان على الائتمان الرقمي

يعني الائتمان Credit إضافة مستقبلة للأموال المشمولة بالحماية بحيث تضمن هذه الإضافة كل التصرفات المالية للشخص. والمبدأ الأساسي في الائتمان هو الحماية، إذ برز الائتمان على إثر تصاعد حدة جرائم السرقة بالإكراه، والتي وصلت إلى أعلى معدلاتها في العدوان على الحياة في مقابل نهب المال من الضحايا. فالهدف يظل هو اختلاس الأموال إلا أن السارق فضلا عن كونه يستخدم الإكراه فإنه كذلك يفضل ألا يترك أثرا وراءه يمكن أن يقود إليه.

وعلى الرغم من كون قاعدة الحماية هي الأموال فإن الجريمة استطالت أيضا الائتمان لكون إن الأموال عبر الائتمان تتحول إلى أرقام موضوعة على كروت يستلمها المؤتمن من المصرف الذي يتعامل معه.

ومن حيث الطبيعة فإنه يميز في شأن الائتمان بين التعامل به في العالم المادي وبين التعامل به الإنترنت. فهو في عالمنا المادي يعد وسيطا لكونه يحل محل النقود في التعامل، حيث أنه عبر الإنترنت لا يمكن اعتباره وسيطا، وإنما هو أحد أشكال السداد كالنقود تماما. ذلك إن ما يتم عرضه للسداد عبر الإنترنت ليس الكارت الذي يثبت وجود الائتمان وإنما رقم التعامل الائتماني الموضوع على الكارت ويسدد به الثمن.

ويتطور التقنية في ظل ثورة المعلومات نشط الائتمان، سيما عبر التجارة الإلكترونية/ الإنترنت على وجه التحديد. فالتعامل المالي عبر الإنترنت كما أنه استطاع استيعاب فكرة ظهور أشكال جديدة للنقود، فإنه كذلك يستطيع استيعاب فكرة الائتمان، خاصة إذا علمنا أن التعامل بالائتمان عبر الإنترنت له سوابق تاريخية. إذ يكفي أن تضع اسمك ورقم بطاقة الائتمان الخاصة بك لكي تصل إلى مبتغاك أو غرضك التجاري

كالبيع والشراء والاشتراك في مؤسسات وأندية...الخ. ويمتد نشاط التعامل بهذه البطاقات إلى النواحي العالمية؛ إذ يجوز اختراق الحدود بمقتضى الائتمان[1] أو بالأحرى تقلص فكرة رقابة الدولة عليها[2].

وفي الفقرات التالية سوف نتعرض لموقف عدد من التشريعات المقارنة من هذه الجريمة ونتطرق بعد ذلك لمظاهر العدوان على الائتمان عبر الإنترنت.

أولا: الجريمة في التشريع المقارن:

كان التشريع الفرنسي من أوائل التشريعات التي قررت سلوك المسلك الجنائي حال العدوان الإجرامي على كروت الائتمان، وذلك منذ العام 1988 بقانون Godfrain (نسبة إلى النائب الذي تقدم بمشروع القانون إلى الجمعية الوطنية) المؤرخ 1988/1/5، وهو القانون الذي أضيف إلى نص المادة (5-462 عقوبات فرنسي جديد) بشأن الاحتيال Faux على بطاقات الائتمان. ومما تجدر الإشارة إليه أن الاحتيال المذكور Faux قد تولى المشرع الفرنسي تفسيره على ضوء المادة (1-441- عقوبات فرنسي جديد). ويشار هنا إلى القانون المؤرخ 30 سبتمبر 1991 المعدل للمرسوم المؤرخ 1935/10/30 بإصدار قانون الصك قد أضاف موادا تتعلق ببطاقات الائتمان وذلك بالعقاب على تقليد Contrfacon وتزييف Falsification هذه البطاقات.

ثانيا: مظاهر العدوان على الائتمان عبر الإنترنت:

تتخذ أشكال العدوان على الائتمان عبر الإنترنت أحد شكلين:

(1) د. حازم الببلاوي: النظام الاقتصادي الدولي المعاصر، عالم المعرفة، العدد 257/الماء/ مايو 2000، الكويت، ص154.

(2) المرجع السابق، ص165.

(أ) الاستيلاء على أرقام كروت الائتمان:

إذ أن لكل كارت ائتمان عنوانا فرديا خاصا ID number يتميز به عن غيره، تمنحه المؤسسة المالية للمشترك لديها في هذه الخدمة بحيث تحل محل التعامل بالأموال السائلة.

والشكل المادي لكروت الائتمان يتمثل في تلك البطاقات البلاستيكية الموصوفة بمقاييس معينة، وأما نطاق استخدامها فيختلف بحسب نوعية الخدمة التي تستخدم فيها. فكما أن هناك بطاقات تستخدم لسحب مبالغ مالية من آلات توفرها المؤسسات المالية التي تصدر هذه البطاقات، فإنه أيضا تتوافر خدمة التعامل بالبطاقة مباشرة في الحياة الاقتصادية من خلال رقم البطاقة.

ولقد امتد نشاط بطاقات الائتمان إلى الإنترنت فانفتح المجال لها لكي تضع عملية استخدامها في محك على درجة عالية من الخطورة إزاء مظاهر الاحتيال التي يتم بها الاستيلاء على أرقام هذه البطاقات بشكل غير مشروع، وعلى النحو الذي يحقق تكامل جريمة الاستيلاء على كروت ائتمان.

وعلى الرغم من أن الاستيلاء على كروت الائتمان عبر الإنترنت يكون بغرض الحصول على سلع وخدمات يتم سداد مقابلها المادي من كروت الائتمان المختلسة، إلا أن موضوع اختلاس كروت الائتمان لا يشكل سرقة مادية أساسا وإنما يكون عدوانا على الائتمان تحديدا باستغلال قيمة الضمان من قبل من ليس له الحق فيه، إذ أن المال المضمون بالائتمان لم تخرج حيازته ماديا على وجه التحديد، وإنما كل ما في الأمر أنه يتم إنفاقه لصالح الغير ممن لا يجوز له إنفاقه دون إرادة

صاحبه. وعليه فنقطة التفاعل في الائتمان هي مسألة الإنفاق ومدى جوازه، وليس الحيازة المادية كما السرقة، ويفيد الائتمان في منطق الإنفاق عبر الإنترنت عدم لزوم الحضور المادي لأشخاص التعامل المالي وهو ما يطلق عليه البعض مصطلح "Carding" والذي يفيد الاستخدام غير المصرح به لكارت الائتمان من قبل مالكه[1]. ومن ثم فإن ما تتم سرقته عبر الإنترنت ليس هو كارت الائتمان لعدم توافر الوسيلة المادية وإنما فقط كود الكارت لذلك يطلق على هذه الجريمة أحيانا مصطلح سرقة الهيئة "Identity theft".

وعلى الرغم من أن اتجاها فنيا يذهب إلى أن الحيازة غير المشروعة لأرقام كروت الائتمان التي تتم عبر الإنترنت إنما هي على درجة كبيرة من الصعوبة، كعملية تقنية تحتاج إلى برمجة معقدة، وبالتالي تعد حركة الحيازة المادية لها أسهل بكثير من حيازتها عبر الإنترنت فإن حالات اختلاس هذه الأرقام عبر الإنترنت من الخطورة بمكان وهو ما دفع المشروع الفيدرالي الأمريكي إلى عدها جريمة وفق 18 7)(U.S.C. 1030(a)(1)[2]. فقد حدث في عام 1996 أن تم اختراق حاسوب محمول LAPTOP يحتوي على 314.000 رقم لكروت ائتمان تخص أحد المكاتب التابعة لمؤسسة Visa Card INT في كاليفورنيا، وفي عام 1997 قام Carlos Sadalgo Jr. (37 عاما) باستخدام حاسوب في جامعة سان فرانسيسكو واختلس أسماء مالكي وأرقام log-ons عدد 100.000 كارت ائتمان وكذلك بيانات أخرى من خلال اختراقه

(1) Dr. Andrzej Adamski (Nicholas Copernicus University, Toran, Poland). Crimes Related to the computer network, threats and opportunities: A criminological perspective OP-CIT, P.221.

(2) Ibid.

لمجموعة مزودي خدمات إنترنت ISPs وقام بوضعها على اسطوانة مضغوطة CD ثم قام بتشفيرها وعرضها للبيع بمبلغ مائتين وخمسين ألف دولار، ولقد اكتشف عملاء المباحث الفيدرالية هذه الجريمة وحوكم سادالوجو وعوقب بالسجن ثلاثين شهرا[1].

(ب) العدوان على التوقيع الإلكتروني:

يعد التوقيع Signature من الأهمية بمكان في كافة المعاملات، فهو التعبير الأمثل عن أصالة كل وثيقة، فأي مستند لا يتضمن توقيعا لا يحمل بذاته إمكانية تفاعله مع القانون على أية شاكلة. والمحاكم لا تعتد بمجرد ورقة مكتوبة بخط اليد، إنما لكي تأخذ هذه الورقة حظها من الاعتبار القضائي فإنه يجب أن تكون ممهرة بتوقيع صاحبها Signatory وبذات اليد التي كتبتها Manuseript signature ومثل هذا الأمر تقليد إنساني معروف منذ القدم. ونتيجة لكثرة تداول التوقيع ولزومه في نسبة أي وثيقة

(1) The CFAA makes it a crime for an unauthorized user to access a computer that is federally owned or is a « protected computer » for the purpose of 1) obtaining records from a bank, credit card issuer, or consumer reporting agency ; 2) committing fraud or extortion ; 3) transmitting destructive viruses or commands ; 4) trafficking in stolen passwords ; or 5) threatening to damage a computer system in order to extort money or other things of value. A « protected computer » is a computer 1) used exclusively by a financial institution or the United States Government ; 2) used on a nonexclusive basis but where the conduct affects use by the financial institution or the government ; or 3) used in interstate or foreign commerce or communication. This last element is intended to keep the federal government out of purely local computer crimes, but the multistate nature of Internet transmission suggests that almost any Internet activity will amount to « interstate commerce ». see : James Garrity & Eoghan Casey. Internet Missue in the Workplace : A Lawyer's Primer, op. cit., at 14.

إلى مصدرها الشخصي فقد أهمل التشريع تعريف مصطلح التوقيع، إلا أنه نتيجة للتطورات الحادثة في القانون المعاصر على أثر خروج تكنولوجيا المعلومات إلى الوجود، وجدت الحاجة لتعريف محدد للتوقيع لكونه اصطبغ بالصفة الإلكترونية، حيث تستخدم الآلة في إعداده، وهو الأمر الذي ترتب عليه بالضرورة لزوم تحديد الوضعية التي يكون عليها مع لزوم شموله في الوضعية الإلكترونية بالحماية القانونية سيما في جوانبها الجنائية. ولقد قنن المشرع المقارن هذا الأمر للدلالة على أهمية التوقيع، فالمشرع الأمريكي تضمن تعريفا للتوقيع في مشروع قانون التجارة (Uniform Commercial Code (UCC حيث يعد توقيعا "كل رمز معتمد بقصد التعبير عن الأصالة".

والتوقيع الإلكتروني كأحد مظاهر التوقيع عامة كان – ولا يزال – أحد اهتمامات المشرع المقارن، ومن ذلك المشرع الأوروبي الذي أصدر توجيها في عام 1995 للشروع في تشكيل لجنة خبراء لكي تتولى وضع مشروع التوقيع الإلكتروني، وفي 16 الصيف/ يونيو 1998 تقدمت اللجنة بمشروعها هذا مقترحة إصدار مجلس أوروبا توجيها بالخصوص، وفي 22 الطير/ إبريل 1999 وضع المشروع النهائي للتوجيه، ولقد قام البرلمان الأوروبي في 12 الكانون/ ديسمبر 1999 بإعداد نصوص التوجيه المذكور ليخرج علينا في ثوبه الأخير.

ولقد أصدر المشرع الألماني قانون الإنترنت لسنة 1997 يتضمن مجموعة نصوص حول الإنترنت المؤرخ في 22 يوليو 1997 ومن بينها نصوص تتعلق بالتوقيع الإلكتروني.

كذلك اعترف المشرع الفرنسي بالتوقيع الإلكتروني حيث تنص المادة (1316-4) من القانون المدني الفرنسي بعد تعديلها بالقانون رقم 230-2000 المؤرخ 13 مارس 2000 حيث تقرر بأن التوقيع الإلكتروني يعد

وسيلة تعامل معترفا بها، ومفترضا صحته Pésumée إلى حين إثبات العكس. ولقد صدر المرسوم التنفيذي لهذا التعديل رقم 272-2001 المؤرخ 2001/3/30 بشأن تطبيق المادة (4-1316) من القانون المدني الفرنسي المتعلقة بالتوقيع الإلكتروني، حيث تضمن في المادة (1/1) تعريفا أكثر تحديدا للتوقيع الإلكتروني بأنه "معطيات ناتجة عن استعمال طريقة ردا على شروط معرفة في صدر الجملة المقررة في الفقرة الثانية من المادة (6-1316- مدني)".

وفي إطار النظام القانوني الإنجليزي استطاع القضاء الإنجليزي في قضية Goodman V. J. Eban. Ltd تحديد الأصالة Authentication بالإضافة إلى مناهج التوقيع الإلكتروني. على إن الأمر لم يقف عند هذا الحد وإنما قامت إدارة التجارة والصناعة الإنجليزية Department of Trade and Industry في مارس 1999 بإصدار وثيقة استشارية Consultation Document بعنوان Building Confidence in Electronic Commerce تم هيكلتها على ضوء التوجيه الأوروبي المشار إليه أعلاه، وبناء على هذه الوثيقة أصدر البرلمان الإنجليزي قانون الاتصالات للمملكة المتحدة المؤرخ 2000/5/25 The UK Electronic Communications Act الذي ينص في القسم (7) من على تعريف للتوقيع الإلكتروني[1].

---

(1) Section 7(1) provides: In any legal proceedings:

(a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and

(b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data, See: Chris Reed-What is a signature?, op. cit., at 15.

وأما المشرع البلجيكي فقد أصدر القانون المؤرخ 20 أكتوبر 2000 الذي أضاف إلى القانون المدني البلجيكي المادة (2281) مقررا الاعتراف بالتوقيع الإلكتروني إلى جوار اعترافه بالتوقيعات التي ترد عبر الفاكس والبريد الإلكتروني والبرقيات والتلكس وبأية وسيلة أخرى[1].

أما المشرع الأمريكي فقد اهتم اهتماما كبيرا بموضوع التوقيع الإلكتروني لكونه أداة فعالة في حركة المعاملات المدنية والتجارية، وتحديدا كان للمشرع الولائي الأمريكي الأسبقية في هذا الإطار، حيث أصدر مشرع ولاية Utah في عام 1995 أول تشريع للتوقيع الإلكتروني The digital signature act of 1995 الذي تم إلغاؤه وإعادة إصدار تشريع آخر في عام 1996، وكان من بين الأغراض التي سعى مشرع ولاية يوتا الأمريكية بإصداره هذا التشريع هو التخفيف من حدة الاحتيال بالتزوير والنصب على التوقيعات ككل[2]. ثم تلا ذلك ولاية كاليفورنيا بقانون 5 سبتمبر 1995 الذي، بعد أن اعتبر التوقيع الإلكتروني في مرتبة التوقيع المادي، قام بتعريف التوقيع الإلكتروني في القسم (5-16) من كود الحكومة الولائية The Government Code بأنه "تحديد إلكتروني للهوية تم إعداده بواسطة الحاسوب ومعتمد من قبل مستخدمه

---

(1) 20 OCTOBRE 2000, Loi introduisant l'utitisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire.

والمادة (2281- مدني بلجيكي) هي المادة التي كان المشرع البلجيكي قد ألغاها بمقتضى القانون المؤرخ 1949/12/15. ولقد أعادها إلى الحياة في ثوب جديد بمقتضى القانون المؤرخ 2000 السالف.

(2) William E. Wyrough, JR & Ron Klein- The electronic signature act of 1996: Breaking down barriers to widespread electronic commerce in Florida, op. cit., at 429.

لكي يكون له ذات القوة والأثر للتوقيع المادي أو اليدوي ولكن لا يشمل هذا التعريف إمكانيات التشفير"[1]. ولتتولى بعد ذلك مظاهر الاهتمام بالتوقيع الإلكتروني من قبل المشرع الولائي الأمريكي مثل تشريع ولاية أويامنغ Wvoming لعام 1995، ثم تشريع ولاية واشنطن Washington الصادر في 2 مارس 1996 الذي اعتمد على تشريع ولاية يوتا، ومما تجدر الإشارة إليه أن تشريع واشنطن تقرر نفاذه مع الأول من شهر يناير 1998.

ولكن ما هو التوقيع الإلكتروني تحديدا، وما هو دوره في الحياة الاقتصادية الاجتماعية عبر الإنترنت وما هي الاستفادة المرجوة منه إزاء تطلب وجوده في حركة المعاملات، وفوق هذا كله هل تكفي النصوص الحالية لكي تتفاعل مع ظاهرة التوقيع الإلكتروني وبحيث تشمله بالحماية الكاملة؟

1- تعريف التوقيع الإلكتروني:

تعددت محاولات تعريف التوقيع الإلكتروني فاختلف الرأي بشأن تحديد تعريف موحد له، وإن كان يظل مظهر الاتفاق الوحيد – رغم الاختلاف – ممثلا في ضرورة توافر طرف ثالث Third Party يطلق عليه سلطة تصديق التوقيع Certification Authority ، والتي يتشابه عملها مع السلطة التي تكون للمصارف حال حجز مبالغ مالية لصالح المستفيد من إصدار الصكوك.

وفي إطار الاختلاف حول تعريف التوقيع الإلكتروني فإن هناك من يرى أن التوقيع الإلكتروني مجرد تسجيل إلكتروني E. Record، وهناك

(1) « An electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual this definition does not include encryption. Further, signature », id at 431.

من جعل التوقيع الإلكتروني يرتقي إلى مستوى الهوية الإلكترونية E. Identity، وثالث استشعر مدى خطورة التوقيع الإلكتروني ليرى فيه صيغة تكنولوجي لها طابع ذاتي من حيث الأصالة E-signature is generic techneutral term لما له من القدرة على التداول العالمي بصرف النظر عن اعتبارات الحدود الدولية، بل أن هناك من يرى إن التوقيع الإلكتروني إن هو سوى معالجة رياضية Mathematical Process تميز الوثائق الإلكترونية من حيث نسبها إلى أصحابها.

أما التوجيه الأوروبي المؤرخ 1999/12/12 المشار إليه فقد انطلق في محاولة منه لاحتواء موضوع التوقيع الإلكتروني لكي يضع تعريفين له أحدهما موسع والآخر مضيق، فالتعريف الموسع هو ما قررته المادة (1/2) من التوجيه بقولها "بيان في شكل إلكتروني يتفاعل بشكل منطقي مع البيانات الإلكترونية الأخرى وله طابع الأصالة كمنهج". وفي المادة (2/2) من التوجيه قرر المشرع الأوروبي "تعني عبارة توقيع إلكتروني متقدم، كل توقيع إلكتروني يتقابل مع أحد المتطلبات الآتية:

(أ) أن يكون مرتبطا كلية بصاحبه.

(ب) أن يكون مؤهلا للتعريف بصاحبه.

(ج) أن يكون متميزا بما يسمح لصاحبه من بالتحكم فيه.

(د) أن يكون مرتبطا ببيانات ذات علاقة به بحيث يكون كل تغيير في البيانات المذكورة غير مقبول.

على أن التعريف الأمثل لدينا هو التعريف الذي يرى في التوقيع الإلكتروني أنه "مجموعة من الحروف أو الأشكال أو الرموز التي تبرز إلكترونيا لها ذات الأثر الذي يحدثه التوقيع المادي"[1]. فمثل هذا التعريف يضع فكرة التوقيع Signature في موضعها الصحيح – عندنا – من

(1) Thomas, Ruth, op. cit., at 4.

حيث أنها عبارة عن اسم شخص الموقع Signatory على الشيء المكتوب من قبله في نهاية ما هو مكتوب[1]، مع ما يشمل ذلك من عدم تحديد لما إذا كان الشخص طبيعيا أم معنويا، وهو التطور الذي قاده المشرع الأوروبي في هذا الإطار وفق ما قرره في توجيه 1999 في المادة (3/2) منه التي قررت أن عبارة الشخص كما قد يكون طبيعيا فإنها أيضا تشمل الأشخاص المعنوية في هذا الإطار.

كما يفيد هذا التعريف في تمييز التوقيع الإلكتروني عن التشفير والذي هو سلسلة من الخوارزميات التي ينبغي تبادلها مع الآخرين، في حين أن التوقيع الإلكتروني يخص الشخص ذاته فهو مالكه وليس للغير أن يتعامل به ولا يحدث بشأنه تبادل من أي نوع كما لا يعد انقسام التعامل فيه مبدأ يحكمه.

وللتوقيع الإلكتروني فائدة كبيرة عبر الإنترنت وبصفة خاصة في نشاط التجارة الإلكترونية، فهو يخفف من حدة الاستخدام الورقي في الاتفاقات ثم إنه يسمح بقدر من المرونة في المعاملات أيضا لكونه يجتاز مسألة الوقت فيختصر الزمن والمسافات أيضا، إذ يكفي أني ضع الشخص توقيعه لكي تتم المعاملات دون حاجة لانتقاله إلى الأماكن المختلفة لكي يقوم بمعاملاته. ولعل أبسط الأمثلة التي تتعلق بالتوقيع الإلكتروني هي تلك التي يمكن اعتمادها في المصارف حيث تتطلب المعاملات المصرفية وجود توقيع معترف به وبدونه المعاملة تماما. ويفيد التوقيع الإلكتروني في كونه يسهل كثيرا العمليات المصرفية.

---

(1) William E. Wyrough JR & Ron Klein, The electronic signature act of 1996 : breaking down barriers to widespread electronic commerce in Florida, op. cit., at 419.

على أن المشرع المقارن لم ينته إلى اتفاق في مسألة تحديد الحماية القانونية والجنائية الواجبة للتوقيع الإلكتروني، فهناك اتجاه تشريعي يجعل التوقيع الإلكتروني في مستوى التشفير، وبالتالي ما ينطبق على التشفير من حماية قانونية ينطبق عل التوقيع الإلكتروني أيضا، وذلك مثل تشريع كاليفورنيا. على أن هذا الاتجاه في الحقيقة لا يتناسب مع ما هو مقرر في ذات التشريع من استواء التوقيع الإلكتروني بالتوقيع اليدوي من حيث القيمة القانونية والآثار التي تترتب على التوقيع. ولعل هذا الأمر هو الذي جعل المشرع الأوروبي يتجه متجه الاعتراف بعدم تمييز التوقيع الإلكتروني عن غيره كاليدوي مثلا، مقررا أن التوقيع كما قد يكون ماديا أو يدويا فإنه من الممكن أن يكون إلكترونيا أيضا. لأجل ذلك وضع المشرع الأوروبي تمييزا في تعريف التوقيع الإلكتروني سواء في صيغة عامة أو في صيغة مخصصة، فالصيغة العامة تفيد اعتراف المشرع الأوروبي بالتوقيع الإلكتروني في حين أن الصيغة المخصصة تفيد في تحديد مدى إمكانية امتداد الأثر القانوني للتوقيع حين يكون إلكترونيا بحيث يصلح - إذا توافرت الخطوات اللازمة - أن يكون نافذا أمام الجهات الرسمية كأن يكون دليل إثبات أمام القضاء مثلا، وهو الأمر الذي قررته المادة (2/5) من التوجيه الأوروبي.

2- مظاهر العدوان على التوقيع الإلكتروني:

كان توجه المشرع الأوروبي هو الانطلاق من اعتبار التوقيع الإلكتروني من البيانات الشخصية، لذلك لم يتوان عن التقرير بمسئولية مزود خدمات توثيق التوقيع الإلكتروني prestataire de service de certification حال قيامه ببث التوقيع أو تسليمه لغير مالكه وهو ما قررته المادة (6) من التوجيه المذكور.

ولكي يتم العدوان على التوقيع الإلكتروني فإن ذلك يأخذ شكل العدوان على الأساليب الآمنة التي يتولاها طرف ثالث محايد Neutral Third Party، هو مقدم خدمات الإنترنت Online Service Provider OSPs، وذلك بالعدوان على وسائل التشفير الضرورية من مفتاح عام وآخر خاص. على إن الأمر قد يأخذ شكلا آخر أكثر سهولة يتمثل في حالة تتبع التوقيع الإلكتروني لشخص ما، بما يستدعي الأمر هنا لزوم إحداث اختراق تام من خلال معرفة الخادم المشترك فيه هذا أو ذاك الشخص، ثم القيام بعد ذلك بالبحث فيه عن الهوية الإلكترونية IP الخاصة بذلك الشخص، حتى يتوصل إليها ثم بعد ذلك القيام باستنساخ التوقيع الإلكتروني خاص به.

3- نقد فكرة التوقيع الإلكتروني بحلول فكرة البصمة الإلكترونية:

أن الاتجاه المعاصر نحو إقرار واعتماد التوقيع الإلكتروني يعد من الموضوعات التي تعد محل نظر، سيما إزاء ارتباط فكرة التوقيع الإلكتروني بفكرة أخرى، لا تزال بعد في طور النمو، وهي فكرة التجارة الإلكترونية. فهذه الأخيرة تعد من الموضوعات التي تعاني في القانون من مسألة تقويمه في الوقت الذي يعاني منها القانون من حيث اتصاله بها، وفيما إذا كان يعد العدوان على التوقيع الإلكتروني عدوانا على الأموال أم على التشفير أم على الحق في الحياة الخاصة...الخ.

فإذا أضفنا إلى ذلك منطق الوسيط الإلكتروني الضامن لفكرة التوقيع الإلكتروني بمقتضى إقرار أو شهادة إلكترونية Le certifical Electronique التي تتعدد أنواعها عبر الإنترنت، والتي بمقتضاها يتم اعتماد التوقيع الإلكتروني فإن ذلك يقودنا بالضرورة إلى أن مسألة التوقيع الإلكتروني يمكن أن تعد من المشكلات إزاء الدقة التي عليها مسألة التوقيع الإلكتروني هذه وما قد تثيره من مشكلات.

ولقد ازداد الأمر تطورا حال بروز فكرة البصمة الإلكترونية التي تتفق في التصنيف مع فكرة وحدانية التوقيع في العالم المادي. إذ أن البصمة الإلكترونية تعتبر عن وحدانية التوقيع من حيث نسبته إلى شخص واحد فقط. وتتخذ البصمة الإلكترونية هنا ذات الشكل التي هي عليه في العالم المادي فقد تكون على هيئة وضع بصمة الإصبع أو العين أو الأسنان أو الصوت...الخ، إلا أنها في كل الأحوال – سواء في العالم المادي أو الافتراضي – فإنها تحتاج إلى الآلة لإقرارها، فمثلا من يريد الاتصال بحسابه المصرفي عبر الإنترنت، فإن الأمر لا يتطلب سوى وضع البصمة الإلكترونية على ماسح ضوئي خاص مرتبط بالحاسوب الذي يوصلها بحاسوب المصرف المذكور... وهكذا.

ومثل هذا الاتجاه الجديد يمكن أن يكون أكثر ثقة في التعاملات المالية لما تتمتع به بصمة الإنسان من ذاتية خاصة، حيث كل إنسان له بصمته الخاص. والعدوان على البصمة كما يمثل تزويرا لتوقيع حيث تقوم البصمة مقام التوقيع إن لم تكن أقوى تأثيرا منه، فإنه يمكن أن يكون الأمر كذلك عبر الإنترنت، حيث يقوم مقلد التوقيع بتزوير آليته.



المبحث الثاني
جريمة الاحتكار والاحتكار المضاد

الأصل دائما أن التجارة حرة لا يقيدها قانون ولا يؤثر فيها سوى حركة المستهلك. وهذا الأصل الاقتصادي لا يوجد سوى في خيال الاقتصاديين دائما، إلا أنه يمثل دائما نقطة الانطلاق الأولى في حركة تنظيم الاقتصاد، وبحيث يعد دائما من الآمال التي أن تتحقق حتى في صبغة المدافعين عن مبدأ حرية التجارة. ذلك أنه طالما وجد القانون الاقتصادي حتى في صيغته العرفية، كان ذلك مؤشرا على وجود قيد على المنافسة في إطار حركة السوق.

وحركة السوق تعني في إطار حرية التجارة والاقتصاد أن مبدأ المنافسة يمتد إلى كافة القطاعات الاقتصادية دون منازع بما في ذلك براءات الاختراع[1]. وإذا كان الاحتكار هو السيطرة على معدلات الاقتصاد في ظل نظم السوق التي تتبع اقتصاديات العرض والطلب، لكونه يتعارض مع مدلول الحرية الاقتصادية، وكذلك القوة الكامنة في التجارة من حيث كونها تعبر عن ذاتها، في منطق فرض هيمنة المنتج الأفضل لدى المستهلك النهائي، فإن عبارة الاحتكار المضاد تعد أخطر مجالا في هذا الإطار، لكونها تمثل استنهاض الهمم لمواجهة العدوان على حركة اقتصاديات السوق الحرة بأقوى الأسلحة الاقتصادية على الإطلاق

(1) 35 USC Sec. 211 Relationship to antitrust laws : Nothing in this chapter shall be deemed to convey to any person immunity from civil or criminal liability, or to create any defenses to actions, under any antitrust law. SOURCE (Added Pub. L. 96-517, Sec. 6(a), Dec.12, 1980, 94 Stat, 3027). REFERENCES IN TEXT : The antitrust laws, referred to in text, are classified generally to chapter 1 (See. 1 et seq.) of Title 15, Commerce and Trade.

والممثلة تحديدا في... الترويج المجاني للسلع كنوع من الرد الاقتصادي على مساهمة حركة الإنتاج في الصراع الخفي الدائر في إطار اقتصاديات السوق الحرة. ويبرز مثل هذا الصراع، أكثر ما يبرز، في إطار صناعة الحاسوب والإنترنت.

وإذا كان الاحتكار المضاد قد برز في أقوى صورة على يد الكبار في مجال الحاسوب، وتحديدا في محاولات شركة مايكروسوفت للرد على القواصم التي تجتاح اقتصاديات إنتاجها من قبل العديد من الشركات مثل AOL (التي امتلكتها Time Warner في نهاية عام 2000) إلا إن ذلك لا يعني عداد الاحتكار المضاد متميزا عن الاحتكار في صورته التقليدية، بل هو في الحقيقة ضرب منه، إن لم يكن وليده، وهو في هذا المنحى تتوافر له مقومات عدم المشروعية.

على إن عدم المشروعية هنا لم ينتظمها قانون متفرد، وإنما ظلت القوانين المجرمة للاحتكار هي المسيطرة حتى على الاحتكار المضاد استنادا إلى ذات الطبيعة التي عليها الاحتكار والاحتكار المضاد، والحقيقة لقد كشفت قضية مايكروسوفت موضوع الاحتكار المضاد بشكل لم يسبق له مثيل، حيث كشفت هذه القضية علاقات السوق الخفية والصراع الباطني حول من يسود؟

وإذا كان مقصد المشرع، في كل دولة تنتهج منهج الاقتصاد الحر، هو السعي إلى خلق المنافسة الكاملة كمقياس لحركة هذا الاقتصاد، فإن لعبة الاحتكار المضاد يمكن أن تكون على درجة عالية من الخطورة، وسلاح فتاك تضر في النهاية بالمستهلك النهائي الذي يستفيد من صراع المنافسة دائما.

والقاعدة التي تحكم الاحتكار هي البحث دائما عن مجال متكافئ للمنافسة في حركة التجارة وبحيث ينشأ الاحتكار دائما حين يتواجد

عدوان على المنافسة. ويلزم المنافسة أن تتصف بالمشروعية دائما، فإذا وجد ما يفيد المنافسة هنا فإن ذلك مؤشر على دخولها في حركة الاحتكار المضاد.

أولا: الاحتكار والاحتكار المضاد عبر الإنترنت

لقد برزت العديد من المشكلات فيما يتعلق بالاحتكار والاحتكار المضاد والإنترنت، ولقد برز هذا الأمر تحديدا في مشكلات أخذت الطابع البسيط ثم تطورت لتأخذ حظها الكبير من الرؤيا القانونية. وإذا كان المشرع المقارن يتجه إلى حصر الإنترنت في المجال القانوني، في محاولة منه لتقييد السلوك السلبي عبر الإنترنت، فإن هذا التقييد يعد احتكارا قانونيا في الحقيقة، وليس احتكارا عدوانيا أو إجراميا. ومثل هذا الأمر يجعل منطق حصر المشرع المقارن لمجموعة من الأعمال، وكذلك تحصين بعض المؤسسات من قاعدة الاحتكار، إنما هو من الأمور اللازمة في هذا الشأن، فالمشرع الأمريكي يرى في اللجنة الفيدرالية للاتصالات FCC مؤسسة مشروعة، ولا يمكن تشبيهها بمزود خدمات أو غيره من مؤسسات الإنترنت، وكذلك فعل المشرع الفرنسي في اللجنة الوطنية للاتصالات CNIL. فمثل هذه المؤسسات لا تعد محتكرة لحركة الاتصالات في مجال تكنولوجيا المعلومات، وإنما هي في الحقيقة ذات أغراض محددة، وأهم هذه الأغراض تسيير العالم الافتراضي تقنيا دون سيطرة عليه في هذا الشأن، ويبرز ذلك في الأثر الكبير الذي صاحب تعديلات قانون الاتصالات الأمريكي لسنة 1934 بالقانون الصادر في 1996، حيث توسعت تلك التعديلات في منح صلاحيات مزودي الخدمات عبر الإنترنت.

وإذا كان الاحتكار كمصطلح يأخذ في مجراه التحكم في حركة العرض والطلب في نظرية السوق، فإن الاحتكار المضاد يعني

بالضرورة العدوان على المنافسة Anti Competation أثناء اشتعالها في السوق من حيث الواقع العملي، بحيث يكون الأمر قد برز على أثر صراعات تنافسية حول منتج أو البحث في القدرة على الاستحواذ عليه فيما يتعلق بحركة التوزيع أو الاستهلاك، وفي هذه الحالة الأخيرة لا يكون المستهلك حرا في اختياراته وإنما يلجأ إلى جهة واحدة تكون قد سيطرت على سوق التوزيع. لذلك فإن الاحتكار المضاد له ذات المضار التي تكون للاحتكار فيما خلا أن المنتج يكون فعلا في السوق وينتج عن سلسلة من السلوك غير الشروع بقصد السيطرة عليه. ويمكن إعطاء مثالا حيا عن الاحتكار المضاد في عام 1999 عند قيام شركة Intel صاحبة أشهر معالجات مصغرة Microprocessors في العالم بالرد اقتصاديا على المنافسة بالإبقاء على منطق حجب التقنية والتأثير في الأسعار، كنوع من الثأر والانتقام من عملائها ممن هم حاصلون على امتيازات براءات اختراع Patents لديها[1] كونهم قاموا بممارسة ضغوط اقتصادية عليها حين رفضوا القيام باستصدار تراخيص منها، على أثر اشتعال سوق المعالجات العالمية.

ثانيا: الجريمة في التشريع المقارن

إن موضوع الاحتكار والاحتكار المضاد أو العدوان على المنافسة من الموضوعات التي أخذت حظها في إطار المفاهيم الاقتصادية للقانون. فقد نبتت الفكرة في القانون المقارن في مجال التفسير الاقتصادي تحديدا، وما توصل إليه القانون العام الإنجليزي English Common Law،

(1) William J. Bear & David A. Balto-Antitrust Enforcement & High Teconoloy Markets, April 30, 1999, Telecommunications & Technology Law Review Vol. 73/1999, P.7, available online in March 2000 at http://www.mttlr.org/volfive/balto.html.

حيث استمد مفهوم الاحتكار Monopoly ومكافحة الاحتكار Anti-Monopoly منه دعما للمنافسة Competition على أسس مشروعة. ولقد قامت الولايات، صاحبة الاختصاص الأصيل في القانون العام الأمريكي، بتقوية نظم المنافسة فيها على أسس مكافحة العدوان على المنافسة المشروعة، ومنهج التحالفات الكبرى، وذلك وفق مفاهيم القانون العام فيها والمستمدة مبادئه من النظام الأنجلوفوني. ومن ذلك كسر حدة الاحتكار لدى كبار المحتكرين في العصر حديث من أمثال Rockefeller صاحب مؤسسة Stanford Oil of NJ التي امتلكت (90%) من مصافي النفط، كما سيطر على حركة نقل النفط العالمي مع نهاية القرن التاسع عشر.

ولقد كان ذلك دافعا إلى نشاط حركة المشرع الأمريكي في اتجاه المحافظة على منهج القانون العام في تنمية المنافسة المشروعة، مع ترك منهج مكافحة العدوان على المنافسة المشروعة للتشريع، فكان أن وافق المشرع الفيدرالي في عام 1890 على مشروع قانون كان قد تقدم به عضو الكونجرس تشيرمان، ولقد أطلق على هذا التشريع قانون تشيرمان The Sherman Act نسبة إليه، وهو القانون الذي تم ضمه إلى القسم الخامس عشر (15 US Code 1) من التقنين الأمريكي. ويعد قانون تشيرمان عصب سياسة مكافحة الاحتكار في الولايات المتحدة الأمريكية، وهو القانون الذي لحقه قانون كلايتون (15 US Code 12) The Clayton Act وقانون لجنة التجارة الفيدرالية ,The Federal Trade Commission Act 15 U.S.C. 41 الذين صدرا في العام 1914. ويتضمن قانون تشيرمان ركيزتين: إذ بمقتضى القسم الأول منه تم إعلان عدم مشروعية العقود والاتفاقات التي تقيد من التجارة مثل التعاقدات التي تؤدي إلى الاحتكار أو الدمج Combination المؤدي إلى قيام الاحتكار

أو التآمر Conspiracy بين الأشخاص الاعتبارية بقصد الاحتكار والتحكم في الأسعار، في حين يحظر القسم الثاني الاحتكار والشروع في الاحتكار.

أما قانون كلايتون – المعدل لقانون تشيرمان السالف – والذي تم تعديله لاحقا بمقتضى قانون روبنسون باتمان في العام 1939. وكذلك قانون سيلير كافوفر في العام 1950، يتعامل مع أربعة أشكال من الأنشطة ذات العلاقة بالمال والأعمال وهي: تمييز الأسعار price discrimination (Sec.2) والاتفاقات والتنظيمات المقيدة exclusive dealing and tying arrangements (Sec.3) والاندماج mergers (Sec.7) ومركزية الإدارة وتشابك العمل الإداري Interlocking directorates (Sec. 8).

أما قانون لجنة التجارة الفيدرالية FTC فقد تضمن ما يفيد مكافحة الوسائل غير العادلة في المنافسة في التجارة ما بين الولايات، والأعمال المضللة في الأنشطة التجارية حيث عدت غير مشروعة.

ثالثا: الاحتكار عبر الإنترنت

مما سلف يمكن القول إجمالا أن الاحتكار يطلق عليه في مفهوم الدول التي تعتنق مفهومه أنه تعبير عن كفاح القانون الجنائي ضد نظرية المؤامرات الاقتصادية Conspiracy Theories، على أن السؤال يظل هنا مرتبطا في هذه الدراسة بمعرفة مدى إمكانية حضور الاحتكار عبر الإنترنت، وفيما إذا كان لمبدأ المنافسة المشروعة وجود في العالم الافتراضي. ومثل هذا التساؤل أجاب الفقه عليه بالإيجاب مقررا إن الاحتكار له وجود عبر الإنترنت، ويبرز ذلك تحديدا في برمجيات الحاسوب وبرمجيات الإنترنت والتي تلحق بالضرورة بالحاسوب لكي يمكن تنفيذها عبر الإنترنت، سيما فيما يتعلق بتطبيق قواعد قررها القضاء المقارن، مثل قاعدة اليد المغلولة The Hands-off Rule.

أننا إذا استثنينا لجنة الاتصالات الفيدرالية ودورها في عملية الاتصالات في العالم الرقمي فإنه يمكن القول أن الاحتكار عبر الإنترنت برز في المنافسة غير المشروعة التي قادها مجموعة شركات كبرى في مجال تكنولوجيا المعلومات وعلى رأسها مايكروسوفت الأمريكية. حيث يمكن القول إن الاحتكار عبر الإنترنت نشط في اتجاه حرب المتصفحات Browser Wars، تلك الحرب الشرسة التي بدأت في ولاية نيويورك ثم امتدت إلى العالم أجمع، وشغلت الرأي العام العالمي، سيما وإنها تمس كبرى شركات البرمجيات العالمية والتي تملك زمام الأمور في نظم التشغيل الأكثر شعبية، والتي على رأسها برامج التشغيل، والبيئة التكنولوجية الأكثر شعبية، برمجية النوافذ Windows. فهي القضية التي جعلت المسؤول الأول في الشركة Bill Gates يصرخ في أحد مقالاته بعبارته الشهيرة قائلا (أو مستجديا) Why they're doing this?.

ولكن ما هي الأسس التي استند إليها القضاء الأمريكي في إدانة شركة مايكروسوفت وإصدار ذلك الحكم القاسي بتفكيكها إلى شركتين منفصلتين. ثم ما هي العوامل التي جعلت المحكمة الاستئنافية تنتهي إلى نقض حكم أول درجة المذكور! وهنا نجد إنه من اللازم أن نتعرض لهذه القضية لكونها تمثل أولى القضايا في حرب المتصفحات عبر الإنترنت.

رابعا: قضية مايكروسوفت[1]

بشكل موجز بدأت وقائع هذه القضية عندما نشطت مايكروسوفت في تحديث متصفحها بعد خروج نظام النوافذ 95، سيما وإن شركة AOL America On Line كانت قد بدأت نسبيا في الترويج لمتصفحها

(1) تولى الادعاء في هذه القضية السيد Joel Klein وكيل النائب العام في جرائم الاحتكار، وأما القاضي فقد كان السيد Thomas Penfield Jackson المسمى قاضيا في عهد Reagan.

الشهير Netscape NN Navigator الذي كان يعد الأكثر رواجا آنذاك، وهو الأمر الذي استشعرت معه مايكروسوفت خطورة موقفها حيث إن البيئة التي يعمل فيها NN هي بيئة النوافذ. ونتيجة لصراع خفي بين شركات أخرى (مثل Intel صاحبة المعالج الشهير المسمى باسمها وSun Microsystems صاحبة برمجية JAVA وهي شركات كانت على علاقات تعاقدية مع مايكروسوفت، قامت الأخيرة باتخاذ خطوات جدية وسريعة وعملية باتجاه تطوير متصفح الإنترنت المملوك لها Internet Explorer (والملحق ببرمجية النوافذ) وبصدور النسخة المطورة من برمجية النوافذ 98 أعلنت مايكروسوفت إن إصدار النسخة المطورة من متصفحها Explorer سوف يكون مجانيا، كونه من ملحقات برمجية النوافذ أصالة، وهو الأمر الذي جعل شركة AOL ورئيسها آنذاك Stave Case يشتاط غضبا، يسانده في ذلك مجموعة من الشركات كانت تأمل أن ترى مايكروسوفت تتهاوى نتيجة لرؤيتها الخاصة حول تنمية فكرة تكنولوجيا المعلومات، وعلى النحو الذي يجعلها أكثر شعبية مما هي عليه، والتي أفصحت عنها منذ خلافها الأول مع شركة IBM في ثمانينات القرن المنصرم.

ذلك الذي سلف كان ملخص الأحداث التي دفعت إلى اتهام مايكروسوفت بالاحتكار، وعندما رفعت الدعوى إلى القضاء - عن طريق ادعاء نيويورك - ليقول كلمته فيها في 1998/10/19، كان محك الصراع القضائي لكي يمكن التوصل إلى الصيغة التي يتم بمقتضاها تحديد الطابع الاحتكاري لـ. مايكروسوفت هو الإجابة على الأسئلة الثلاثة التالية:

- النظر فيما إذا كانت مايكروسوفت تملك قوى احتكارية Monopoly Power في سوق نظم تشغيل الحاسوب الشخصي PCOSs؟

- النظر فيما إذا كانت مايكروسوفت دخلت في علاقات قوية مع غيرها لحماية هيمنة نظام التشغيل Windows من المنافسة، باستخدام نهج عملي منظم؟
- النظر فيما إذا كان نشاط مايكروسوفت قد أساء إلى الابتكار وكذلك إلى المستهلكين؟

(أ) القوة الاحتكارية لمايكروسوفت:

وهذه تمثل النقطة الأولى المشار إليها أعلاه. ولقد لوحظ فيما يتعلق بالقوة الاحتكارية لشركة مايكروسوفت تلك القدرات الكبيرة لديها في السيطرة على المعالجات المتوافقة Processes Compatible لشركة Intel، وهي المعالجات التي يمكنها جعل الحاسوب يعمل بكفاءة لا تصل إلى المستوى الذي تحققه حواسيب متكاملة مثل حواسيب IBM وCompaq مثلا، إلا أن هذه المعالجات جعلت سوق الحاسوب يتسع للقاعدة الشعبية حول العالم. ونتيجة لوجود هذا المعالج في السوق التجارية فإن مايكروسوفت سيطرت على (90%) من نظم التشغيل في العالم[1].

(ب) سلوكيات مايكروسوفت:

قامت مايكروسوفت بسلوك مسلك الأعداد لحرب طويلة الأمد ضد مؤسسة AOL مالكة المتصفح NN آنذاك، حيث قامت مايكروسوفت بإنفاق الوقت والجهد والمال على تطوير متصفحها IE، ثم بعد ذلك قامت بترويجه مجانا، مما جعل ذلك السلوك يبدو مقيدا لتكنولوجيا المعلومات. كما صدر عن مايكروسوفت سلوكا يتضمن بذاته وسيلة ضغط على بعض الشركات، مثل تهديدها الكتابي لشركات مثل شركة Compaq

(1) Stephen Tolbert, op. cit at 3.

بإلغاء ترخيص Intel إذا لم يتم تحميل متصفح مايكروسوفت المتطور IE على نظام التشغيل Windows في حواسيبها. كذلك عندما رفضت شركة IBM الشهيرة عرض مايكروسوفت بتطوير نظم التشغيل Windows قامت الأخيرة بمعاقبتها برفع أسعار الترخيص المذكور. كما سارت مايكروسوفت على ذات المنوال بالنسبة للعديد من الشركات التي تعمل في مجال الحوسبة مثل Real Network, Sun Microsystems, Appel.

(ج) الإساءة إلى المستهلك:

يعد ما قامت به مايكروسوفت مظهرا من مظاهر مكافحة المنافسة Anti-Competitive كونها قيدت المستهلك النهائي، وهو المستخدم لنظام التشغيل، وحقه في الاختيار[1]، سيما وإن المستهلك المذكور يرتبط بنظام التشغيل هذا طالما أنه يستخدم الحاسوب برمجة وعملا وإبحارا عبر الإنترنت أيضا، بحيث لن يكون له الحق في وجود اختيارات تسمح بالمنافسة كحد أقصى أو أنها تسمح بعدم الاحتكار في الحد الأدنى.

ومما سلف فإن مايكروسوفت بدأت في مسلك الاحتكار من حيث أنها قامت بشكل غير مشروع بربط متصفحها IE في نظام تشغيلها Windows 98 وذلك يشكل انتهاكا للقسم الأول من قانون تشيرمان، كما أنها قامت بالسيطرة على سوق متصفحات الإنترنت Web Browser Market بالمخالفة للقسم الثاني من قانون تشيرمان. حيث إن مايكروسوفت بذلك حاولت السيطرة في سلوكياتها هذه على سوق تكنولوجيات البرمجة بربطها بنظام تشغيلها، بالشكل الذي يجعله مصدر الحياة الكامل لكل برمجية يمكن أن يقوم الغير بإعدادها، وهو ما جعل

(1) Stephen Tolbert, op. cit at 2.

القضاء يرى في ذلك انتهاكا للمعايير التي تحكم الاستهلاك والمستهلك عن طريق تحديد الأسعار Price Fixing[1]، مما يجعل مايكروسوفت تقع تحت طائلة القسم الثاني من قانون تشيرمان.

لذلك كله اتجه قضاء أول درجة[2] إلى الإقرار بإدانة مايكروسوفت، وذلك بفرض عقوبة علاجية عليها، حيث استلزم في هذه العقوبة فرض منهج المنافسة عليها بقوة القانون، وذلك بفصل خط إنتاج البرمجيات في شركة مايكروسوفت عن خط إنتاج نظام التشغيل فيها بما يجعل الانفصال انفصالا قائما بين عمل الحاسوب وبين عمل الإنترنت. وإنشاء ثلاث شركات لبرمجية النوافذ كل منها مستقلة عن الأخرى استقلالا كليا في إطار الملكية الفكرية وبحيث يكون لها أيضا استقلالية الالتزام على أن الانتصار الكبير الذي حققته الحكومة الأمريكية ضد مايكروسوفت لم يستمر طويلان فقد نقضت محكمة الاستئناف حكم أول درجة في 2001/6/28 (محكمة الاستئناف لمقاطعة كولومبيا)، لأسباب تتعلق بعدم ثبوت الاحتكار بحيث بدا الأمر لمحكمة الاستئناف هنا كما لو كانت المنافسة ليست للسيطرة على سوق المتصفحات وإنما احتدم الجدل حول بيئة النوافذ التي تحتاج إلى مجهودات شركات أخرى في الوقت الذي تملك مايكروسوفت هذه البيئة في تشغيل الحواسيب، وبما يجعل الغير في حاجة إلى مايكروسوفت، ومثل هذا الأمر يخضع لإرادة الشركات الأخرى وليس لإرادة مايكروسوفت التي تملك مثل هذا المنتج الناجح

(1) Price Fixing among competitors is a horizontal restraint and a per se violation of the Sherman Act. See : Shawn W. Potter, op. cit at 20.

(2) US v. Microsoft Corp, 56 F. 3d 1448 (D. C. Cir. 1995) (« Microsoft 1 »). See also : United States v. Microsoft Corp., 147 F. 3d 935 (D.C. Cir. 1998) (« Microsoft II »).

شعبيا، وكان من ضمن هذه الأسباب ما يتعلق بصلاحية قاضي المحكمة لكونه خالف نظام القضاء المقرر في القسم U.S.C. Sec. 455(a 28)، بقيامه بالتصريح للصحافة أثناء نظره للقضية[1].



(1) US. V. Microsoft Co., App. Colombia No. 00-5212, 00-5213 (No. 98cv01233), June 28, 2001.

المبحث الثالث
جرائم الأخـلاق

إن التعرض لجرائم الأخلاق عبر الإنترنت ليس بالموضوع السهل، إذ يجد الباحث ذاته في إطار هذه النوعية من الجرائم عرضة لبحث الاختلاف الاجتماعي على المستوى الأخلاقي والقائم بين الحضارات، بل وحتى بين المجتمعات في الدولة الواحدة، فيبرز له بصورة منطقية إن هناك اختلافا في طبائع المجتمع ومستويات النظرة الفردية الاجتماعية إلى الأمور لكونها ترتبط بمفهوم المدنيات المعاصرة. وارتباطها كذلك بمنطق أو نهج التعامل مع الإنسان في المجتمع. فما يكون معد انحلالا أخلاقيا في حضارة أو دولة أو مجتمع معين قد لا يكون كذلك في نهج دولة أخرى، وقد يختلف في نهج دولة ثالثة... وهكذا.

لذلك فإنه يلاحظ أنه وإن كان ليس هناك بد من التطرق إلى هذه النوعية من الجرائم حين تتم عبر الإنترنت، فإن ذلك لا يعني سوى التطرق إلى الحلول التي طرحها المشرع لهذه النوعية من الجرائم، من حيث كونها شكلت مشكلة ذات شأن كبير، على الرغم من حركة الإباحة الأخلاقية التي تجتاح بعض المجتمعات غير الإسلامية.

وجرائم الأخلاق وفقا للتصنيف المصلحي في قانون العقوبات هي تلك النوعية من الجرائم التي تتضمن العدوان على القيم الأخلاقية المتعارف عليها في النظم الاجتماعية الاقتصادية.

ويعد العدوان في جرائم الأخلاق من ضمن أشكال العدوان على القيم الإنسانية الاجتماعية، مع ما يصاحب هذا الأمر من تشدد في الطابع الحضاري لتلك القيم، والمستوحى - هذا التشدد - مما تعارف عليه الناس وارتضوه قاعدة أخلاقية، وهو أمر يفترض تباين الحضارات والثقافات في المستوى الأخلاقي، إذ من الممكن أن يكون ما هو غير أخلاقي في

حضارة معينة معاصرة معد أخلاقيا في حضارة أخرى معاصرة أيضا. وإذا كان ذلك صحيحا إلا أن ذلك لا يعني عدم وجود حد أدنى لقواعد أخلاقية يمكن أن تكون أساسا لقانون عقوبات عالمي مستوحى من الأخلاقيات الذاتية للشعوب.

ولقد أولى المشرع المقارن اهتماما ملحوظا بالجرائم الأخلاقية، وفقا لما تمليه عليه حضارته كما أسلفنا، وذلك يعني تحديدا إن الاختلاف الحضاري لا يؤدي إلى نزع الأخلاق من الحضارات، وإنما تختلف النظرة إليها من حضارة إلى أخرى فحسب. فالمشرع الليبي رصد الجرائم الأخلاقية في الباب الثالث من الكتاب الثالث من قانون العقوبات لسنة 1953 في المواد من (407) إلى (424) ثم إنه يرتب آثارا على ارتكاب مثل هذه النوعية من الجرائم في التشريعات الأخرى، لكون العامل الأخلاقي في ليبيا مستمدا من الحضارة الإسلامية الرشيدة ومنطق التقاليد التي تأسس عليها هذا المجتمع في إحداث البنية الأخلاقية هناك. وذات الأمر ينطبق على التشريع المصري وكذلك التشريع الصادر في الدول العربية والإسلامية، في حين انه في التشريع الصادر في الدول غير العربية وغير الإسلامية فإن الحال أن المشرع يستمد المعيار الأخلاقي من المنطق الاجتماعي الاقتصادي لديه، إلا أن ذلك لا يعني انعدام تواجد العامل الأخلاقي، بل أنه كثيرا ما يلاحظ قوة العامل الأخلاقي هناك، وعلى أساسه تقوم فكرة الحقوق المدنية هناك.

- العلنية والعرض للجمهور والمصطلح الأخلاقي عبر الإنترنت:

إن العدوان على الأخلاق عبر الإنترنت يعد في الحقيقة من المشاكل جعلت الاصطدام قويا بين المشرع والقضاء في القانون المقارن، ولقد احتلت مشكلة الأخلاق عبر الإنترنت حيزا كبيرا في بحوث الفقه المقارن، في عملية صراع كبيرة ما بين حرية التعبير واحترام أخلاقيات

الشعوب. إذ أن المشرع المقارن لا يتوانى عن سن التشريعات التي تحمي القواعد الأخلاقية، إلا أن القضاء المقارن يقوم بإلغاء هذه التشريعات سعيا وراء حماية حرية التعبير، كإحدى الحريات التي تتفوق على الأخلاق. ومع ذلك فإن المشرع، كردة فعل، يقوم مرة أخرى بإعادة سن التشريعات بغرض حماية الأخلاق، بحيث مثلت القاعدة الأخلاقية على هذا النحو تحديا بين المشرع والقضاء في القانون المقارن.

وفي هذا الفرع سوف نتعرض لثلاثة موضوعات دقيقة في مضمونها حين الارتباط بالإنترنت وهي موضوعات العلنية والعرض للجمهور والمصطلح الأخلاقي عبر الإنترنت لكونها أثارت جدلا في القضاء المقارن.

أولا: شرط العلنية

العلنية Publication وصف لحالة حدث أو عمل أو نشاط يباشره الشخص في حدود القانون. فليست العلنية قيمة في ذاتها وإنما تبرز تلك القيمة في مدى تأثيرها في الحدث بحيث تجعله ينتقل بمقتضى هذا التأثير إلى الجمهور، وبحيث يترتب على وصفه بالعلنية نتائج يعترف بها القانون ويرتب عليها آثاره.

وقد ينص المشرع في تشريعه العقابي على نص عام يحتوي منطق العلنية ينطبق على كافة الجرائم، مثلا هو الحال فيما هو مقرر في المادة (1/16- عقوبات ليبي) التي تنص على أنه تعد الجريمة مرتكبة علنية إذا كان ارتكابها: (أ) بطريق الصحافة أو غيرها من وسائل الدعاية والنشر، (ب) في محل عام أو مفتوح أو معروض للجمهور وبحضور عدة أشخاص، (ج) في اجتماع لا يعد خاصا نظرا للمكان الذي انعقد فيه أو لعدد الحاضرين أو للغرض الذي عقد من أجله"، ويعد مثل هذا النص قاعدة عامة تضمنها القسم العام من قانون العقوبات يتم تفسير كلمة العلنية

كلما وردت في النصوص على ضوئها. ولا يعني رصد قاعدة عامة تؤدي دورها كتعريف أو تحديد امتناع المشرع عن رصد معنى مخصص للعلنية، بل يمكنه القيام بذلك كما هو الشأن في المواد (284-286- عقوبات ليبي)[1].

ولعل المثار في مقصود العلنية المدى الذي عرض له المشرع الجنائي هنا، وبالتالي أنواعها المشار إليها، لاسيما فيما يتعلق بالفرق بين المحل العام أو المفتوح أو المعروض للجمهور وبين عبارة الاجتماع الذي لا يعد خاصا نظرا للمكان الذي انعقد فيه أو لعدد الحاضرين أو للغرض الذي عقد من أجله. وهذا يقود بالضرورة إلى القول بأن كل اجتماع خاص، بالنظر إلى المكان الذي أعد فيه أو لعدد الحاضرين أو للغرض الذي أعد من أجله، يجعل العلنية منتفية عن الواقعة، كما هو الشأن في الاجتماع الذي يعقد في منزل ما للعائلة إذا حدث وتبادل بعضهم البعض عبارات قذف وسب، ففي هذه الحالة لا تتوافر العلنية.

(1) تنص المادة (284- عقوبات ليبي) على أنه "يعاقب بالحبس مدة لا تزيد على سنة وبغرامة تتراوح بين عشرين ومائة دينار أو بإحدى هاتين العقوبتين كل من أذاع بطريق الصحافة أو بأي طريق آخر من طرق العلانية بيانا عن قضية جنائية نظرت سرا أو أذاع محتويات وثائق أو أوراق تتعلق بتحقيق في قضية يجب أن تبقى سرية قانونا. ولا يطبق هذا الحكم على الوثائق وحيثيات التحقيق التي أدلى بها فيما بعد في مناقشة علنية وبوجه عام لا يطبق على سائر أوراق الإجراءات الجنائية القضائية بعد انقضاء ثلاثين سنة على الفصل فيها أو قبل ذلك إذا أذن وزير العدل بالنشر صراحة. ولا يعاقب في الأحوال المنصوص عليها في الفقرة الأولى من هذه المادة على مجرد الإعلان عن القضية ولا نشر الحكم فيها فقط". وتنص المادة (286- عقوبات ليبي) على أنه "يعاقب بالعقوبات المذكورة في المادة السابقة كل من نشر بأي طريقة من طرق العلانية المداولات السرية بالمحاكم أو نشر بغير أمانة وبسوء قصد ما جرى في الجلسات العلنية بالمحاكم".

ومن ثم فإن وجود شبكة داخلية بين أفراد العائلة ليست مرتبطة بالإنترنت وإنما تظل بين أفراد العائلة الواحدة في نطاق مكاني موزع وليس محدد فإنه لا تتوافر به صفة العلنية حال وجود واقعة سب أو قذف، حتى مع إمكانية حدوث الاختراق هنا لكون المخترق مرتكبا لجريمة انتهاء حق الخصوصية ولو كانت الصفة التي تواجد بها هي الحضور مصادفة.

وإذا تأملنا التمييز بين المحل العام أو المفتوح أو المعروض للجمهور وبين عبارة الاجتماع الذي لا يعد خاصا نظرا للمكان الذي انعقد فيه أو لعدد الحاضرين أو للغرض الذي عقد من أجله، فإن القضاء المقارن كان قد تعرض له في محض التمييز بين عبارتي To the public و In the Public، حال التعرض لقانون حق المؤلف، بحيث اعتبرت محكمة الاستئناف الفيدرالية لـ.كيبك/ كندا بأن عبارة To the public أعم من عبارة In the public، فهذه الأخيرة يتناسب مدلولها مع منطق الاجتماع الذي لا يعد خاصا نظرا للمكان الذي انعقد فيه أو لعدد الحاضرين أو للغرض الذي عقد من أجله، في حين أن العبارة الأولى تندمج في فكرة المحل العام أو المفتوح أو المعروض للجمهور، وهو الأمر الذي يترتب عليه القول أنه في الاتصال المباشر فإن المجموعات الإخبارية Newsgroups تعد محلا عاما أو مفتوحا أو معروضا للجمهور حال وجود إمكانية لأي شخص أني لج إليها دون شروط خاصة، في حين تكون هذه المجموعة الإخبارية اجتماعا لا يعد خاصا إذا كان مكان انعقاده على الإنترنت محددا بموقع معين (إذ يستطيع أي شخص أن يستدعيه)، إلا أنه في ذات الوقت يحتاج إلى تحديد هوية وكلمة مرور لكي يمكن للشخص الولوج إلى موقع المجموعة الإخبارية، وفي هذه الحالة فإن الأمر يصير إلى العلنية أيضا، أما إذا كانت المجموعة الإخبارية مرتبطة بشبكة خاصة، وهذا الأمر كثير الحدوث كما لو كان

هناك شركة أو مؤسسة تملك شبكة خاصة بها فإن تداول الأحاديث بنظام المجموعات الإخبارية والاجتماعات المغلقة عبر الشبكة المذكورة لا تتوافر به العلنية، لكون الولوج إليها من قبل الغير، إنما يعد ولوجا غير مشروع طالما لم تتوافر فيه المشروعية الكافية لذلك[1].

وقد لا يرى المشرع ضرورة للنص على قاعدة عامة تتضمن تفسيرا للعلنية، مكتفيا بتحديد مصطلح العلنية في نصوص خاصة معتمدا في تحديد نطاق تفسيرها على ما يقرره القضاء في هذا الشأن. مثلما هو حال المشرع المصري في المادة (171- عقوبات مصري) التي تنص على أنه "كل من أعرى واحدا أو أكثر بارتكاب جناية أو جنحة يقول أو صياح جهر به علنا أو بفعل أو إيماء صدر منه علنا أو بكتابة أو رسوم أو صور شمسية أو رموز أو أية طريقة أخرى من طرق التمثيل جعلها علنية أو بأية وسيلة أخرى من وسائل العلنية يعد شريكا في وقوع تلك الجناية أو الجنحة بالفعل. أما إذا ترتب على الإغراء مجرد الشروع في الجريمة ليطبق القاضي الأحكام القانونية في العقاب على الشروع. ويعتبر القول أو الصياح علنا إذا حصل الجهر به أو ترديده بإحدى الوسائل الميكانيكية في محفل عام أو طريق عام أو أي مكان آخر مطروق أو إذا حصل الجهر به أو ترديده بحيث يستطيع سماعه من كان في مثل ذلك الطريق أو المكان أو إذا أذيع بطريقة اللاسلكي أو بأية طريقة أخرى. ويكون الفعل أو الإيماء علنيا إذا وقع في محفل عام أو طريق عام أو في أي مكان آخر مطروق أو إذا وقع بحيث يستطيع رؤيته من كان في مثل ذلك الطريق أو المكان. وتعتبر الكتابة والرسوم والصور الشمسية

(1) Commission du droit d'auteur – Canada, Public Performance of Musical Works 1996, 1997, 1998 – Public Performance of Musical Works – Copyright Act, Section 67.2, October 27, 1999, P.29.

والرموز وغيرها من طرق التمثيل العلنية إذا وزعت بغير تمييز على عدد من الناس أو إذا عرضت بحيث يستطيع أن يراها من يكون في الطريق العام أو أي مكان مطروق أو إذا بيعت أو عرضت للبيع في أي مكان".

وفي النص الأخير يلاحظ أن المشرع المصري سوى في التجريم بين القول العلني والإيماءة العلنية والفعل العلني والكتابة العلنية...الخ. فالقول هو الصوت ويمكن أن يكون مصدره مباشرا كما هو الشأن في جريمة السب وقد يكون غير مباشر كما هو الشأن في التشهير عبر الصحف أو في الإذاعة. والإيماءة هي الإشارة، والفعل هو الحركة العضوية العلنية مادامت تتضمن تعبيرا ما، والكتابة هي التدوين بلغة مفهومة قصد التعبير عن فكرة أو موضوع ويلحق بها الرسوم والصور الشمسية والتصوير الخيالي كالكاريكاتير والتصوير المرئي والرمزي[1]. وقد تكون الكتابة بطريق النشر وقد تكون مراسلة خاصة، إلا أنه نظرا لطبيعة الوسيلة التي تم بها الإرسال تكون قد استقرت في إطار العلنية، كما هو الشأن حين إرسال فاكس أو برقية...الخ، بحيث يكون قد اطلع عدد من الناس عليها قبل وصولها إلى المجني عليه. على أن السؤال هنا يتعلق بالبحث عن مدى أهمية تطلب العلنية في جرائم الأخلاق للقول بإمكانية قيام التجريم في مثل هذه الأحوال. ذلك أن بعض جرائم الأخلاق تتم في السر، بل وإنها تشترط السرية كواقع، وما دور القانون هنا سوى البحث في مدى وقوعها لكي يرتب عليها نتائجه.

والواقع أن العلنية ذات شأن في بعض جرائم الخلاق وليس كلها مثلما هو الحال في الفعل الفاضح العلني والبث الفاضح أو الفاحش العلني

(1) د. جميل عبد الباقي الصغير: الإنترنت والقانون الجنائي، الجوانب الموضوعية، المرجع السابق، ص68.

والتعرض لأنثى (420 مكرر – عقوبات ليبي) التي تنص على أنه "يعاقب بالحبس مدة لا تقل شهر ولا تزيد عن ستة أشهر كل من تعرض لأنثى على وجه يخدش حيائها بالقول أو الفعل أو الإشارة في طريق عام أو مكان مطروق. وكل من حرض المارة على الفسق بإشارات أو أقوال أو أفعال. وتكون العقوبة الحبس مدة لا تقل عن شهرين ولا تزيد عن سنة إذا عاد الجاني إلى ارتكاب جريمة من نفس نوع الجرائم المشار إليها في الفقرة السالفة خلال سنة من تاريخ الحكم عليه، ولا يجوز في هذه الحالة الأمر بإيقاف تنفيذ العقوبة المحكوم بها".

ولما كانت الإنترنت من وسائل العلنية – بطبيعتها – فإن ذلك يقودنا إلى ضرورة بحث هذه المسألة، إلا أننا سوف نتجه إلى رصد البحث في العلنية عبر الإنترنت في كل حالة على حده، سعيا وراء التقرير بأن العلنية عبر الإنترنت ينبغي تطلبها لكون الأفعال التي تعد جريمة عبر الإنترنت كثيرة ومتنوعة، بما يعني أن العلنية متطلبة حال تطلب المشرع لها وبحيث لا تكون العلنية شرطا عاما ينبغي توافره كلما كان هناك جريمة عبر الإنترنت.

ويلزم ذلك بالطبع التعرض للمصطلحات القانونية التي يستخدمها المشرع المقارن لتحديد الفعل اللاأخلاقي عبر الإنترنت، ثم تطرق إلى التشريع المقارن ودوره في رصد الإجرام الأخلاقي عبر الإنترنت وذلك كتمهيد إلى تحديد الجرائم الأخلاقية في هذا المطلب.

مسألة العرض للجمهور

ورد مصطلح العرض للجمهور في القانون الليبي في معرض المادة (1/16-ب- عقوبات) حيث قرر المشرع إمكانية عداد الجريمة مركبة علانية إذا ارتكبت في محل معروض للجمهور، في حين قرر المشرع

المصري منطق العرض للجمهور في البابا الرابع عشر من قانون العقوبات، في المواد (171) وما بعدها، سيما المادة (178، ثالثا/2- عقوبات مصري) التي رددت مصطلح "وكل من أعلن عنه أو عرضه على أنظار الجمهور". ففي الحالتين تتوافر العلنية المتطلبة في الجرائم التي يتطلب فيها المشرع لزوم العلنية.

وفيما يتعلق بتحديد الجريمة الأخلاقية التي يمكن أن ترتكب علنا عبر الإنترنت، يمكن القول بأن المصطلح المستخدم في التشريع المصري يمكن أن يحقق نوعا من التوافق مع شبكة المعلومات الدولية/ الإنترنت، بحيث أن ما هو موضوع أو موجود على هذه الشبكة من مواد أي كانت يمكن القول بأنه يتم عرضه من قبل شخص ما على أعضاء (جمهور) الإنترنت، في حين لا يمكن أن تكون الإنترنت محلا معروضا للجمهور، لأن الإنترنت ليست محلان حيث أن مقصود المحل في النص الليبي هو النطاق الجغرافي الذي يجمل على مفهوم الحيز المكاني المادي، في حين أن العرض على الجمهور وفقا للنص المصري لا يستدعي أن يكون المحل الذي تم العرض فيه محلا معروضا للجمهور في معنى الحيز، وإنما كل ما تطلبه المشرع هنا هو العرض على الجمهور بأية وسيلة كانت، سواء كانت في العالم المادي أو في غيره. ولما كانت الإنترنت وسيلة اتصالات جماهيرية فإن المفترض الصحيح، وفقا للقانون المصري دون الليبي هنا، إنه بمجرد وضع المادة المجرمة على شبكة المعلومات الدولية/ الإنترنت تكون قد تم الإعلان عنها أو عرضها على الجمهور، دون حاجة لإقامة الدليل على أن جمهورا قد اطلع على المادة الإجرامية من عدمه.

وعندما أن نص المادة (178، ثالثا/2 – عقوبات مصري)[1] يمكن أن تجد لها مكانا من التطبيق في جرائم الإنترنت، دون نص المادة (1/16-ب- عقوبات ليبي). فمثلا من يسمح للغير بوضع أية مقالة أو أية كتابة من أية نوع عبر أحد صفحات موقعه على شبكة المعلومات الدولية/ الإنترنت، فإنه يكون قد قبل أن يوضع أي شيء مكتوب على موقعه، ويكون صاحب الموقع هنا هو من يقوم بالإعلان عنها أو بعرضها على الجمهور، وفي هذه الحالة تسري عليه نص المادة (178، ثالثا/ 2- عقوبات مصري) في من يعيب في حق ممثل دولة أجنبية معتمد في مصر بسبب أمور تتعلق بوظيفته، وفي المادة (182- عقوبات مصري) عن طرق كتابة إعلان أو مقال، ولو لم يكن صحفيا وإنما يتضمن تشهيرا، ويقوم بوضعه على موقع عبر الإنترنت مسموح فيه بهذا الوضع، لا يكون قد قام هو بالعرض وإنما يعاقب مقترف لجريمة تشهير هنا، كذلك من يرتكب جريمة المادة (1/102- عقوبات مصري) بإذاعة إشاعة من شأنها تكدير الرأي العام وإلقاء الرعب بين الناس وإلحاق

---

(1) تنص المادة (178، ثالثا – عقوبات مصري) على أنه "يعاقب بالحبس كل من صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض صورا من شأنها الإساءة في سمعة البلاد، سواء أكان ذلك بمخالفة الحقيقة أو بإعطاء وصف غير صحيح أو بإبراز مظاهر غير لائقة أو بأية طريق أخرى. ويعاقب بهذه العقوبة كل من استورد أو صدر أو نقل عمدا بنفسه أو بغيره شيئا مما تقدم للغرض المذكور، وكل من أعلن عنه أو عرضه على أنظار الجمهور أو باعه أو أجره أو عرضه للبيع أو الإيجار ولو في غير علانية، وكل من قدمه علانية بطريقة مباشرة أو غير مباشرة ولو بالمجان وفي صورة من الصور وكل من وزعه أو سلمه للتوزيع بأية وسيلة. فإذا ارتكبت الجرائم المنصوص عليها في هذه المادة عن طريق الصحف سرى في شأنها حكم المادة السابقة.

الضرر بالمصلحة العامة إذا أنشأ موقعا على الإنترنت تضمن مثل هذه الإشاعة[1]، فضلا عن ذلك يعاقب مالك الموقع حتى ولو لم يكن هو كاتب عبارات التشهير، ذلك إن مالك أو صاحب الموقع عبر الإنترنت هو الشخص الذي تولى العرض على الجمهور، فما يعاقب عليه القانون وفق هذه المادة هو مجرد العرض على أنظار الجمهور دون أن يكون متطلبا أن يكون العارض هو ممن صدرت عنه مواد العيب.

وعندما يمكن القول بصلاحية هذه المادة للانطباق على الجرائم المرتكبة عبر مواقع تسمح باستخدام صفحات فيها للتعبير عن فكرة أو طرح موضوع من قبل الجمهور، ففي هذه الحالة يظل صاحب الموقع عرضة للمسئولية الجنائية والقانونية عما قد يرتكب من جرائم عبر موقعه إذا لم يتخذ الاحتياطات لمنع مثل هذا العيب وكذلك التدابير الكافية لتصحيح مثل هذه الوضعية وبما ينبئ عن حسن نيته في هذا الإطار.

والسبب الذي يجعلنا نتجه إلى اعتناق هذا الذي سلف، هو أنه مادام قد تسيد الاتجاه القانوني المقام في تنظيم الإنترنت، فإنه لا يمكن أن يتم القبول بالخروج عن النظام الاجتماعي الاقتصادي أو النظام العام عبر الإنترنت، ومن ثم يسري على الإنترنت ذات مقومات النظم الاجتماعية الاقتصادية. ولا يمكن الاحتجاج هنا بعدم معرفة أو علم صاحب الموقع الذي يتضمن صفحة إعلانية مجاني بالمادة المنشورة، حال كونها مجرمة، ففي مثل هذه الأحوال يلزم التقرير بأن مجرد فتح الصفحة للجمهور لكتابة ما يشاء فإن مسئوليته تكون قائمة لقبوله المسبق بهذا الإعلان أو العرض على الجمهور للمادة أيا كانت. ويلاحظ هنا أن القبول

---

(1) انظر محكمة جنح النزهة بمصر - الحكم في القضية رقم 457 لسنة 2002 الموافق 2002/4/11 جنح أمن الدولة طوارئ.

بالإعلان أو بالعرض على الجمهور ليس مفترضا بل أنه واقعي، وهو قائم في الواقع لكون الارتضاء بالإعلان مسبقا يمكن أن يكون له تشابه مع حقيقة من يملك لوحة إعلانات مجانية معروضة على أنظار الجمهور يضع فيها من يشاء أية مواد معيبة في حق الغير، ففي هذه الحالة يكون صاحب اللوحة المذكورة هو من يقوم بالإعلان عن مادة ليست ملكا له وإنما للغير، ومن ثم تقوم المسئولية في حقه حتى ولو لم يكن صاحب المادة معروفا أو كان ممهرا كتابته باسم مستعار. خاصة إذا كان صاحب الموقع المذكور يستغل الصفحات، التي بعدها الغير مجانا، في نشر إعلانات.

المصطلحات غير الأخلاقية التي يتداولها القانون الجنائي:

نتيجة للفارق الحضاري في قوانين الأخلاق والناتج الحضاري الاجتماعي في هذا الشأن، فإن كثيرا من التشريعات يميز فيها بين الفعل غير الأخلاقي Indecency وبين الفحش Obscenity والدعارة المصورة Pornography. ويترتب على هذه المفارقة نتائج شتى في التشريع المقارن، إلا أنها في الواقع الاجتماعي من حيث الاختلاف الحضاري، فإن وقع أو تأثير كل من هذه المصطلحات له أساس يرتبط بمدى الحرية الأخلاقية التي يمنحها المجتمع لأفراده، وإلى أي مدى يمكن أن تصل، بل إنه في بعض التشريعات المقارنة تمكن المشرع من إلغاء التشريعات التي تعاقب على الزنا الإرادي، مثلما هو الحال في التشريع الفرنسي والأمريكي، تاركا مثل هذا الفعل منتظما في إطار ردة الفعل الاجتماعي وأحيانا الديني.

ولعل من موجبات التذكير حين التعرض للتعدد الاصطلاحي في القانون المقارن (بل في إطار كل قانون أيضا) إن المشرع لم يتعرض على الإطلاق لتحديد معنى موحد لمصطلحات الأخلاق الواردة في

القانون الجنائي، ففي القانون الأمريكي قرر القضاء إن مصطلح غير أخلاقي Indecent مصطلح غامض Vague[1]. كذلك لم يرد في على الإطلاق أي تعريف لمصطلح الدعارة المصورة في ذات القانون[2]، ويبرز ذلك واضحا في التوسع الكبير الذي تسير عليه المحكمة الفيدرالية العليا الأمريكية في تحديد مصطلح الفحش Obsecenity، حيث يمكن لهذا المصطلح استيعاب المصطلحات الواردة في القسم 1461 وما بعدها من الباب 18 وكذلك القسم 223 من الباب47 من التقنين الأمريكي[3]، وهي مصطلحات الفاحش Obscene والفسق Lewd والشهوانية Lascivious وكذلك البذاءة Filthy[4]، سيما تلك النصوص التي تتضمن جرائم غير أخلاقية باستخدام الإنترنت والحاسوب[5].

ولقد كان القضاء الأمريكي واضحا في تحديد إمكانية العقاب، بمقتضى القسم (1461)، إذا تم استخدام مصطلحات الفحش بطريق المراسلة، سواء تضمنت هذه المراسلة إرسال كتاب أو بانفليت Pamphlet أو مطبوع Printing أو أية وسيلة إعلانية Publication تحتوي على هيئة لا أخلاقية[6].

(1) Reno V. ACLU No. 96-511 (U.S. Jun 26, 1997), US sup Court.

(2) Herb Lin, PHD hlin@nas.edu , Michele Kipke, PHD mkipke@nas.edu – Tools and strategies for protecting kids from pornography and their applicability to other inappropriate internet content, P.6, Computer science and telecommunicatins board on children, youth, and families, the national academies, available online in dec. 2000 at: http://www.nationalacademies.org.

(3) 18 U.S.C. Sec. 1461 to 1469; 47 U.S.C. Sec. 223.

(4) Roth V. usa, Supp. 354 U.S. 476 (1957).

(5) 18 U.S.C. Sec. 1462, 1465.

(6) Roth v. USA, op. cit.

ولقد تأكد هذا التفسير في عام 1962[1] حيث قررت المحكمة العليا الأمريكية له أنه في إطار الاستخدام العام لمصطلحات الفحش فإنها تتخذ أشكالا مختلفة من المعاني[2]. إلا أن المحكمة العليا عادت في عام (1976) لتضع منطقا جديدا لمصطلح الفحش، حيث رفضت مطلقا التحديد القديم المشمول بالغموض Vagueness Challenge حين تفسير القسم 1461 المشار إليه، وذهبت إلى أن هذه المصطلحات الواردة في القسم المذكور إنما هي مجموعة مصطلحات محددة بشكل ظاهر في وصف السلوك الجنسي Hard Core الذي يعطي كمثال في أثناء الكلام[3]. كما أن القانون الليبي لم يحدد ما هو أخلاقي أو داعر أو فاحش من حيث التعريف، على الرغم من إن القضاء يقوم بدور كبير في رصد القيم الاجتماعية ومدى تفاعلها مع النصوص القانونية في هذا الشأن.

ومثل هذا الأمر يجعل بحث نقاط الاتصال، ومعايير تمييز ما هو أخلاقي وما هو غير ذلك، وكذلك تصنيف الأفعال غير الأخلاقية، من الأمور التي ترتبط بالفهم الاجتماعي الذي يأخذ طابع التعدد حتى في البيئة الواحدة.

لأجل ذلك نجد أن المحكمة العليا الأمريكية استندت حين نظرها قضية Reno v. ACLU، فيما يتعلق بقانون آداب الاتصالات 1996، إلى معيار قاضي المحكمة الابتدائية التي أصدرت الحكم المطعون فيه، وهو القاضي Sloviter، حيث استعان هذا القاضي بمعيار ورد في قضية أخرى هي قضية Sable Communication v. FCC حيث قررت

(1) Manual Enterprises, Inc v. Day, Supp. 370 (1962).

(2) Id "while in common usage the words have different shades of meaning, the statute since its inception has been aimed at obnoxiosly debasing portrayals of sex".

(3) Haming v. USA Supp. 418 U.S. 87 (1974).

المحكمة في هذه القضية الأخيرة أن العبارات الجنسية تعد غير أخلاقية، ولكنها على العكس من العبارات الفاحشة فهي مشمولة بحماية الدستور الأمريكي في التعديل الأول منه.

ولكل ما تقدم فإننا نقول إنه إذا كان هناك مجال لتحديد المعيار الأخلاقي عبر الإنترنت، فإن محاولات القضاء المقارن في هذا الإطار إنما تأتي تعبيرا عن المنطق الاجتماعي السائد، وبحيث يجب الاستعانة هنا فيما هو متعارف عليه في المجتمع ولكن يظل هنا التذكير بأن المنطق الاجتماعي Community Standards له أهمية كبيرة في تحديد عناصر الجريمة الأخلاقية بحيث يتم الاستناد إليه كأساس للبحث في الوقائع.

وربما يعطي مثال استخدام اللهجات العامية العربية وغير العربية - والتي تختلف من محيط اجتماعي إلى آخر، وقد يكون هذا الاختلاف بادي للعيان حتى في إطار الدولة الواحدة - إشارة واضحة المعالم إلى إمكانية التفاعل مع العامل الأخلاقي، بحيث يمكن حين استخدام هذه أو تلك اللهجة أن تفهم على نحو خاطئ من قبل البعض ممن هم ينتمون إلى فئة اجتماعية أو جهة جغرافية قد تكون في ذات الدولة، مثل هذا الأمر يجعل مذهب القضاء الأمريكي له قبول في المنطق والقانون على السواء إذا أدركنا أن المشكلة التي تواجه المشرع والقضاء والفقه هنا يتم التعبير عنها في استحياء شديد سعيا وراء الإجابة على سؤال مقتضاه "أية معايير اجتماعية هي تلك التي يتم تطبيقها".

ولقد أخذ القضاء الأمريكي في الإجابة على هذا التساؤل منحى جديدا بعض الشيء فيما يتعلق بتطبيق المعايير الاجتماعية على جرائم الأخلاق التي ترتكب عبر الإنترنت، حيث أخذ في الاعتبار المعايير الأخلاقية السائدة في المكان المرسل إليه المواد غير الأخلاقية، ثم تطور الأمر أكثر

بحيث قرر القضاء الأمريكي الاستناد إلى معايير ثابتة غير مختلف عليها اجتماعيا كما هو الشأن في دعارة الأطفال مثلا بحيث لا يلتفت القضاء في هذه الحالة إلى بث المعايير الاجتماعية.

ومن الأهمية بمكان الطرق إلى نقطة تفاعل الإنترنت مع الجانب الأخلاقي في الإنسان، فقد أثيرت هذه المسألة بشكل جعل التفاعل التشريعي لازما معها، حتى إن استشعار مدى أهمية التدخل التشريعي يوحي بأن هذه مشكلة لم يكن لها وجود في عالمنا المادي، وإن أول بروز لها كان في العالم الافتراضي/ الإنترنت.

ولقد كان المشرع الأوروبي نشط في نهاية القرن العشرين في مجال حماية الأخلاق عبر الإنترنت سيما بعد قيامه بإصدار التوجيه رقم EC/46/95 المؤرخ 1995/10/24 المتعلق بالتداول الحر للبيانات عبر الإنترنت، فقد أصدر مجلس أوروبا الكتاب الأخضر بشأن حماية القاصرين الذي نشر في شهر أكتوبر 1996.

أما في القانون الإنجليزي فقط أمكن للقضاء هنا التوصل مبكرا إلى طرح موضوع الفحش Obscene، حيث تعرضت محكمة استئناف إنجلترا عام 1997 لمسألة تحديد تفسير لمصطلح الفحش. ولقد وجدت المحكمة في معرض تفسيرها للمصطلحات الواردة في قانون حماية الأطفال لسنة 1978 وقانون علنية الدعارة لسنة 1959، بأنهما لا يلتقيان مع فكرة التراسل الإلكتروني للبيانات The electronic transmission. حيث كان هناك مشكلتان تعترضان القضاء الإنجليزي في التوصل إلى تفسير محدد لهذا المصطلح، وبالتالي تفسير القانونين بما يتفق وتكنولوجيا المعلومات، الأولى وتتعلق بمحتوى النسخة المرئية The Visual Image الموضوعة Stored في ذاكرة الحاسوب، حيث أنها تعد نسخة من الصورة A copy of a Photograph كما هو مقررة في

التشيع، حيث أن المحكمة انتهت في شأنها إلى أنها موضوعة في القرص الصلب، وهي عبارة عن صورة مرئية تم مسحها Scanned[1] من ذلك القرص الصلب لكي يتم تحويلها Transmission إلى قرص صلب في حاسوب آخر، وهي على ذات الشاكلة دون تغيير في هيئتها وبالتالي تنتقل إلى الحاسوب الآخر كما هي A copy of a Photograph لأغراض تطبيق قانون عام 1978. أما المشكلة الثانية فتتعلق بمدى إمكانية وجود تساو Tantamount بين وضع الصور المذكورة في القرص الصلب لحاسوب ما، وبين حركة توزيع هذه الصور. بحيث تختلف نية وضع هذه الصور عن تلك المتطلبة لتوزيعها.

ولقد انتهت محكمة استئناف إنجلترا في حكمها بالإدانة إلى التقرير بأن مجرد وضع شخص ما لصور دعارة في القرص الصلب لحاسوب ما، وبين حركة توزيع هذه الصور. بحيث تختلف نية وضع هذه الصور عن تلك المتطلبة لتوزيعها.

ولقد انتهت محكمة استئناف إنجلترا في حكمها بالإدانة إلى التقرير بأن مجرد وضع شخص ما لصور دعارة في القرص الصلب لحاسوبه فإن ذلك يعني أن هذا الوضع كان بقصد أن يطلع عليها هو، فإذا قام هذا الشخص بفتح حاسوبه للغير فإن ذلك يقاس على حالة فتح مكتبة للإطلاع على محتوياتها، إذ سمح صاحب المكتبة بمن نسخة من المفتاح للغير هنا[2].

وبتعديل كل من هذه التشريعات، بسبب تكنولوجيا المعلومات وتأثيرها على القانون المعاصر، بمقتضى قانون العدالة الجنائية والنظام

(1) Scanning is accomplished by dividing a picture up into little tiny elements called pixels. Sec: David J. Loundy-E-Law S. op. cit at 28.

(2) Id.

العام لسنة 1994[1]، وضع المشرع مصطلحا جديدا هو Pseudo – Photograph المقرر في القسم (7.7) من قانون 1978، والذي يشير إلى الاعتراف بالمنظر/ الصورة Image، التي تم إعدادها بواسطة برمجيات الحاسوب التصويرية أو بوسيلة أخرى، كصورة Photograph[2].

إن الاستفهام الذي يمكن أن يثار هنا يتعلق بالبحث فيما إذا كان هناك تنوع في الجريمة الأخلاقية عبر الإنترنت. وهذا الأمر سوف نتولى العرض له في الفقرة التالية توصلا إلى تحديد تقسيم مصلحي لهذه الجريمة.

إن أشكال الجرائم الأخلاقية عبر الإنترنت تتميز بخصيصة ثابتة تتمتع بها كلها، وهذه الخصيصة تتمثل في أن كافة أنماط الجريمة الأخلاقية عبر الإنترنت تشترك في كونها لا تتجاوز الطابع المرئي/المقروء، وغير المجسم، بحيث لا تسقط في مرحلة الحس الجسدي أو المادي، إلا إذا تحولت هذه النوعية من الجرائم إلى الاتصال المادي العادي بما يستدعي ذلك الخروج من العالم الافتراضي On line والعودة إلى العالم المادي Off Line، لذلك فمن غير المتصور أن تكون جرائم الأخلاق عبر الإنترنت جرائم مادية. وعليه فكل ما يمكن استحداثه من تقسيمات لنوعية جرائم الأخلاق عبر الإنترنت يجعلها كلها تشترك في طريقة تكوينها اللامادي أو المعنوي. ويظل السؤال هنا كامنا في مدى إمكانية تعامل النصوص الجنائية الحالية مع جرائم الأخلاق عبر الإنترنت، وما إذا كانت هناك حاجة لتطوير النصوص المتعلقة بالجرائم الأخلاقية لكي تتوافق مع طبيعتها الرسمية وبحيث لا تكون الإنترنت وسيلة لارتكاب جرائم أخلاقية ويظل مرتكبها في مأمن من العقاب.

(1) The criminal justice & Public Order act.

(2) Id.

ولكي يتم لنا صناعة هذا الطلب فإننا هنا سوف نقوم بإحداث تقسيم مصلحي يتفق مع الإنترنت من ناحية، ومن ناحية أخرى يعبر في الوقت ذاته عن إمكانية احتوائه لمثل هذه النوعية من الجرائم دون عناء الاستعانة بطريقة التقسيم التقليدية التي درج عليها الفقه حين تعرضه لهذه النوعية من الجرائم، وذلك بسبب عدم إمكانية ارتكاب كافة الجرائم الأخلاقية عبر الإنترنت.

إذن في هذا المطلب سوف نتناول بالبحث جرائم الأخلاق الممكن ارتكابها عبر الإنترنت، فليس كل الأفعال الأخلاقية المقررة في قانون العقوبات يمكن ارتكابها عبر الإنترنت، ومثل هذا الأمر يقودنا إلى الإقرار بجزئية أو نسبية جرائم الأخلاق عبر الإنترنت. على أن هذه النسبية أثارت موضوع جرائم الأخلاق عبر الإنترنت بشكل جدلي، فمثلت تلك الجرائم أعتى أشكال الجرائم لما تتمتع به الإنترنت من تحرر رقابي غير مسبوق.

وعليه، يمكن استحداث تقسيم لجرائم الأخلاق عبر الإنترنت بحيث نتعرض لفكرة الترويج السمعي المرئي الفاضح، ثم نتطرق إلى موضوع جرائم البث العلني الأخلاقية من حيث جرائم النشر والقذف والسب والتشهير، ثم ننتقل إلى جريمة المطاردة الأخلاقية التي لها أساس في التجريم غير الأخلاقي وانتقل بعد ذلك إلى التجريم الأخلاقي.



المبحث الرابع
جريمة الترويج السمعي - المرئي الفاضح

أولا: مصطلح الترويج عبر الإنترنت

إن مصطلح الترويج له صبغة العمومية لكونه قد يكون بمقابل أو بغير مقابل، فهو كمصطلح أعم من مجرد البث. والترويج وإن كان مجانيا لا يعني إمكانية قيام الغير بملك منتجات ما، وإنما كل ما في الأمر أن انعدام المقابل إنما يعني انفتاح أو إمكانية وجود قدر من الحرية في استعمال الشيء أو المنتج.

ويمكن أن يتسع الترويج عبر الإنترنت كذلك ليشمل المحادثة الشفهية بأية وسيلة كانت كالتي تتم عبر الفيديو الرقمي أو البث الحي له بطريق الإنترنت أو بطريق الدوائر المغلقة كعرض الشهادة في المحاكم أو تناول موضوعات عامة عن بعد. ولعل أخطر مظاهر الترويج اسمعي المرئي هو أن يلحقه صفة الفضح فيما يصطلح عليه باللغة الإنجليزية بعبارة Cyber Audio – Visual Indecent، فمثلا القيام بالاتصال بالغير باستخدام الإمكانيات السمعية المرئية عبر الإنترنت، مع القيام بحركات أو إيماءات فاضحة، من الأمور التي يمكن أن تشكل جريمة ما هنا، ويزداد الأمر صعوبة حالة وجود نوع من التداول لمثل هذه الحركات السمعية المرئية الفاضحة، من خلال تسجيلها والقيام بتداولها عبر الإنترنت، والمشرع المقارن يهتم في صيغة تقليدية بمثل هذه الجرائم، من خلال التعامل بالفيديو في العالم المادي كما هو الشأن فيما هو مقرر في المادة (1/178- عقوبات مصري)[1] التي امتدت إلى المعاقبة على حيازة

(1) تنص المادة (1/178- عقوبات مصري) على أنه "يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرة آلاف جنيه أو بإحدى هاتين العقوبتين كل من صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض مطبوعات أو مخطوطات أو رسومات أو إعلانات أو صورا محفورة أو منقوشة أو رسومات يدوية أو فوتوغرافية أو إشارات رمزية أو غير ذلك من الأشياء أو الصور عامة إذا كانت منافية للآداب العامة.

شرائط فيديو مخلة بالآداب، سواء كانت هذه الحيازة بقصد الاتجار أو العرض بمقابل أو بدون مقابل[1]. وهو الأمر المعاقب عليه في القانون الأمريكي بمقتضى القسم (18 US Code Sec 2252) التي تعاقب على الاتجار والنقل Transporting والحيازة Possession لبرمجيات حاسوب تتضمن دعارة أطفال[2].

على أنه نتيجة لتنوع أساليب الترويج السمعي المرئي الفاضح عبر الإنترنت، ما بين بث صور فاضحة ووثائق مكتوبة إلى عرض مرئي مختلف الأحجام، إلى ملفات صوتية تروي قصصا جنسية. والغالب الأعم من هذه الأنماط والأنواع يتم بثه عبر شبكة المعلومات الدولية www. إلا أن البعض الآخر يتم ترويجه أيضا عبر الشبكة القديمة كالمجموعات الإخبارية Use net Groups . فقد قام المشرع المقارن بتطوير آلية

---

(1) طعن جنائي مصري رقم 3116 لسنة 55ق جلسة 1987/10/28 المكتب الفني لمحكمة النقض المصرية السنة 38 صفحة رقم 878- ولقد أشارت المادة (2/1) من قانون المطبوعات المصري رقم 20 لسنة 1936 (الوقائع المصرية العدد 23 في 1936/3/2- موسوعات التشريعات العربية) إلى أنه يقصد بالتداول بين المطبوعات أو عرضها لبيع أو توزيعها أو إلصاقها بالجدران أو عرضها في شبابيك المحلات أو أي عمل آخر يجعلها بوجه من الوجود في متناول عدد من الأشخاص. انظر: د. جميل الصغير، الأحكام الموضوعية، السابق، ص89.

(2) USA v.Miller, App 11th Cir No.98-8228, Feb. 4-1999, Available online in March 1999 at: http://www.lp.findlaw.com/scripts/getcase.pl?navby=search&case.../988228man.htm

تشريعه لكي تتواءم مع هذا الأمر كما هو الشأن في التشريع الإنجليزي الذي وسع من فكرة النشر العلني Publication لمواد فاحشة Obscene matter المقررة في قانون الفحش العلني لسنة 1959، بمقتضى قانون لعدالة الجنائية والنظام العام لسنة 1994، لكي تشمل التداول بالحاسوب Computer Transmission لصور Images ونصوص Text[1].

ومن الأشكال ذات الخطورة الخاصة في الترويج السمعي المرئي الفاضح عبر الإنترنت ما تتمتع به هذه الأخيرة من طبيعة اتصالية، إذ يمكن أن يقوم الأشخاص في هذا المجال بتبادل الأحاديث الجنسية، وهو ما يطلق عليه عبارة Cybersex، حيث يكون الحديث بين أشخاص لا يعرف بعضهم البعض، وبحيث يختلف الحال هنا عن الاتصال الذي يجريه الشخص بعاهرات بطريق الهاتف كنوع من الخدمات الإباحية التي تقدم في العالم الغربي في هذا المجال. حيث يمكن لأي أن يقوم بتنظيم نشاط إباحي عبر الإنترنت، كترتيب مواعيد جنسية وكذلك اختيار الهدف الجنسي من خلال العرض المرئي والسمعي مع دفع قيمة ذلك. كذلك يتم عبر الإنترنت الترويج للرقيق الأبيض وتجارة القاصرات ودعارة الأطفال بقصد الاستخدام الجنسي Cyber Teen في الوقت الذي يستمر مرتكب هذه الجريمة في حالة تخف قد لا يكون من السهولة التعرف عليه، خاصة إذا كان يباشر نشاطه عبر المواقع المجانية أو من خلال المجموعات الإخبارية أو القائمة البريدية[2].

---

(1) Conseil Federal suisse: Message concernant la modification du code penal suisse et du code penal militaire (Infractions contre l'integrite sexuelle; prescription en cas d'infractions contre l'integrite sexuelle des enfants et interdiction de la possession de pornographie dure) du 10 Mai 2000, P.7/2775.

(2) لمزيد من التفصيل في هذه القضية انظر الموقع التالي:
http://www.leeds.ae.uk/law/pgs/vaman/watchmen.htm

ومن الوقائع الكبرى في مكافحة جريمة دعارة الأطفال تلك التي تعرف لدى الشرطة الإنجليزية، بعد تدخلها في يوليو 1995 فيها بمصطلح Operation Starburst، حيث اتخذ التحقيق فيه هذه العملية بعدا دوليا، لاسيما وأن الإنترنت في هذه الواقعة قد استخدمت كمجال لدعارة الأطفال وتوزيع صور فاضحة للأطفال، ولقد أدين في هذه الجريمة تسعة رجال إنجليز، كما تم الاستدلال على مجموعة أخرى عبر أوروبا وأمريكا الجنوبية وشرق آسيا وصل عدد المدانين في هذه الجريمة إلى سبعة وثلاثين شخصا[1]. كما قامت المباحث الفيدرالية الأمريكية بالتحقيق في قضية أطلق عليها Innocent Images، وهو التحقيق الذي بدأ على إثر اختفاء طفل أمريكي، من ولاية مريلاند، في العاشرة من عمره. وهي القضية التي أدين فيها 161 شخصا. وفي العام 1997 كانت قضية Operation Rip Cord التي قامت بها المباحث الفيدرالية بالقبض على 1500 شخص من المشتبه فيهم بالتعامل في دعارة الأطفال عبر الإنترنت وبث صور فاضحة Child pornographers للقصر. ولقد قادت عمليات البحث والتقصي حول دعارة الأطفال عبر الإنترنت، في ألمانيا والمملكة المتحدة والولايات المتحدة الأمريكية، إلى الكشف عن مائتي ألف صورة من صور دعارة الأطفال، كما تمت مصادرة مائة وسبعة وثلاثين ألف حاسوب شخصي/ منزلي Home PC. وفي العام 1998 قام البوليس الإنجليزي بعملية كبرى أطلق عليها اسم Cathedral بالتعاون مع الشرطة في 21 دولة في أوروبا وأستراليا والولايات المتحدة والبوليس الدولي الإنتربول لضبط حوالي مائة شخص ممن يتعاملون في دعارة الأطفال عبر الإنترنت.

---

(1) Dr. Andrzej Adamski, op. cit at 223.

وفي شهر أكتوبر 2000 قام المدعي العام الإيطالي بإحالة 1491 من الإيطاليين إلى القضاء، لكونهم قاموا بإنزال download صور دعارة أطفال Child pornography عبر الإنترنت، بعد أن قامت الشرطة الإيطالية بتفتيش ستمائة منزل، وبينهم تسعة أشخاص كانوا يتاجرون في دعارة الأطفال عبر روسيا. وتعد هذه الدعوى الأكبر في إيطاليا في ذلك التاريخ، حيث قام المدعي العام الإيطالي Alfredo Ormanni بإحالة 831 متهما إلى القضاء الجنائي، وتم استدعاء 660 من جنسيات أجنبية ويعتقد أن أغلبهم من روسيا وفرنسا وماليزيا[1].

ثانيا: جريمة الترويج السمعي المرئي الفاضح في التشريع المقارن

اهتمت التشريعات المقارنة بظاهرة الترويج السمعي - المرئي الفاضح، وبصفة خاصة موضوع دعارة الأطفال التي أخذت من المشرع المقارن اهتماما كاملا في هذا الإطار.

في الولايات المتحدة نشط الفقه والقضاء والتشريع في دراسة نظم القانون الأخلاقي وعملية نظمه في القانون الجنائي، على إثر الكارثة الحقيقية الممثلة في دعارة الأطفال عبر الإنترنت، وهي ظاهرة اعتبرت هناك خطرة على المثل القومية التي تقوم عليها دعائم المجتمع الأمريكي[2]! لكون الإنترنت وسيلة تجعل ارتكاب مثل هذه الجرائم سهلا، أو بمعنى أكثر دقة تجعل من الممكن ومن ثم توفر المناخ الملائم للحصول على ضحايا في مثل هذه النوعية من الجرائم. ومثل هذا الأمر

(1) Martin Stone, Italians charge 1491 in online pedophile sting, newsbytes, 30 Oct. 2000. http://www.newsbytes.com/news/00/157391.html.

(2) Herb Lin, PhD hlin@nas.edu, Michele Kipke, PhD mkipke@nas.edu – Tools and Strategies for protecting kids from pornography and their applicability to other inappropriate internet content, op. cit, P.1.

جعل الفقه والقضاء والتشريع في الولايات المتحدة يتجه إلى الاستمرار في دراسة دعارة الأطفال عبر الإنترنت - وذلك بإيعاز من البيت الأبيض الأمريكي في بيانه المؤرخ 1996/1/26 الذي صدر ردا على إلغاء القضاء الأمريكي لنصوص في قانون أخلاق الاتصالات لسنة 1996 المعدل للقانون الصادر في 1936[1].

ونتيجة لمبادرة البيت الأبيض المذكورة فإنه في عام 1998 أصدر الكونجرس الأمريكي القانون رقم Public Law 105-314 بشأن حماية الأطفال من التعدي الجنسي[2]. ولقد تضمن هذا القانون حث النائب العام الأمريكي على التعاون مع الأكاديمية الوطنية للعلوم/ مجلس البحوث الوطنية فيها، على إعداد دراسة متكاملة لبحث مدى إمكانية تفعيل القانون الجنائي في القضايا الأخلاقية، والتي أنتجها التعامل السلبي مع تقنية المعلومات/ الإنترنت. على أن يتم وضع هذا التقرير في خلال سنتين من تاريخ صدور القانون المذكور. ولقد تم وضع التقرير في العام 2000 متضمنا الخطوات الفعالة من الوجهة العلمية من قبل الأستاذين Herb Lin, PhD, Michele Kipke, PhD، بالتعاون مع جهات أخرى ذات علاقة. ولقد وجد التقرير إن مشكلة الدعارة المصورة Pornography ذات أساس من ناحيتين، الأولى كونها تعد داخلة في نطاق اهتمام قسم اجتماعي له دور في المجتمع، حتى وإن كان سلبيا. أما الناحية الثانية فيتعلق بالتحديد القضائي لمصطلح الدعارة الذي يتخذ مفهوم يتسع ليشمل الطابع المتغير فيها vary widely من نطاق اجتماعي إلى آخر Vary by community[3].

---

(1) Reno v. ACLU, US Supp. 521 U.S. 844 (1997).

(2) Protection of children from Sexual predators act of 1998 Title 9 section 901. US Code. Id at 422.

(3) Herb Lin, PhD hlin@nas.edu, Michele Kipke, PhD mkipke@nas.edu – Tools and Strategies for Protecting Kids from Pornography and Their Applicability to other Inappropriate Internet Content, P.4.

ولقد أشار الباحثان في التقرير المذكور إلى أن المشكلة يتم النظر إليها من الزاوية العائلية والمدرسية، وفيها ينبغي أن يكون هناك دورا للعائلة والمدرسة في توعية النشء. ومن الزاوية الاجتماعية على مستوى الدولة وبحيث ينظر إليها كمشكلة تتعلق بـ... سلوك مستهجن Inappropriate content يضم في إطاره كافة أنواع السلوك المستهجن الأخرى والتي يمكن ارتكابها سواء عبر الإنترنت أو غيرها[1]، ومن ثم يجب التعامل مع هذا السلوك المستهجن كظاهرة كلية ليس فيها تمييز فيما لو تمت عبر الإنترنت أو في العالم المادي. حتى في ظل المنطق السائد من حيث لزوم الأخذ في الاعتبار منطق الظروف الاجتماعية في كل بيئة، وفي هذا ما يناقض اتجاهات القضاء الأمريكي في عدم إمكانية حصر أنواع السلوك المستهجن لاختلاف الثقافات، حيث كان ذلك هو السبب في نقض القانون المذكور وبما يعد ذلك عودة إلى نهج قانون أخلاق الاتصالات لسنة 1996 المنقوض.

كذلك يجب الأخذ في الاعتبار ما هو مقرر في القانون الأمريكي من العقاب على توريد Import مواد فاحشة Obscene Material إلى داخل الولايات المتحدة حسبما هو مقرر في القسم US Code Sec. 1462 18. وهذا النص الأخير يقتضي بالطبع أن تكون المواد الفاحشة قد تم إعدادها في خارج الولايات المتحدة الأمريكية، بحيث تصل إلى داخل الحدود الإقليمية بعد ذلك. ومثل هذا النص يثير مشكلتين، إحداهما تبرز حين التعرض لتحديد المواد الفاحشة التي يمكن أن تكون عرضة لمساءلة القانون، وفق هذا النص، سيما وإن هناك درعا قويا ممثلا في مبدأ حرية

(1) Ibid.

التعبير (التعديل الأول للدستور الأمريكي) حتى وإن كان موقف المحكمة العليا الأمريكية هو أن التعديل الأول لا يحمي الفحش. وأما المشكلة الثانية فهي تتعلق بتحديد الدخول إلى الحدود الإقليمية حيث يسري القانون الأمريكي. ذلك إن هذه المواد إذا تم نقلها ماديا فإن ذلك لن يشكل مشكلة في انطباق القانون. وكذلك إذا تم توريدها باستخدام الحاسوب وتم إخراجها منه وتداولها في داخل الولايات المتحدة، إلا أن ما يمكن عده مشكلة يتعلق تحديدا بموضوع البث الآلي للمواقع الفاحشة، حيث أن بث موقع يتضمن مواد فاحشة من خارج الولايات المتحدة فإنه يصل آليا إلى داخل الولايات المتحدة، فهل يعد مثل هذا البث الآلي توريدا إلى داخل الولايات المتحدة؟

كذلك يحظر القانون الأمريكي تصدير Transport المواد الفاحشة ما بين الولايات أو إلى خارج الحدود الفيدرالية (US Code Sec. 1463 18).

كذلك يجرم القانون الأمريكي تشغيل Employ القصر Minors أو دفعهم Induce إلى المشاركة في صور متحركة Visual depiction تتضمن حركة جنسية مباشرة، إذا كان التصوير قد تم باستخدام حاسوب عبر مؤسسات تجارية في الولايات أو في خارج الولايات المتحدة (18 US Code Sec. 2251). كذلك يحظر القانون الأمريكي استخدام الحاسوب لبيع Sell أو نقل Transfer حق الوصايا على قاصر مع العلم بأن هذا القاصر سوف يتم استخدامه لإعداد صور متحركة تتضمن سلوكا جنسيا مباشرا (18 A) US Code Sec. 2251)). كما يجرم القانون الأمريكي استخدام الحاسوب لنقل Transport دعارة الأطفال Child pornography عبر الولايات أو عبر مؤسسات تجارية أجنبية (18 A) US Code Sec. 2252 & 2252))[1].

(1) USA v. Hay, App. 9th Cir. No. 99-30101, 24 Oct. 2000, Available online in Oct. 2000 at: http://laws.findlaw.com/9th/9930101.html.

أما في فرنسا فإن المادة (24-227) من قانون العقوبات الفرنسي الجديد تعد حجر الأساس في إطار دعارة الأطفال[1]. حيث يعاقب معد مواقع دعارة الأطفال وفقا للمادة (24-227) في فقرتها الأولى من ذات القانون، أما الفقرة الثانية منها فتعاقب مستخدم الموقع.

وأما قانون العقوبات البلجيكي فقد تضمن في المادة (383 bis) منه (المضافة بالقانون المؤرخ 1995/4/13) [2] العقاب على عرض Expose وبيع Vendu وتأجير Loue وتوزيع Distribute أو دعم موقع مرئي Remi des supports Visuals لأوضاع جنسية ذات طابع فاحش Pornographique، وذلك باستخدام قصر ممن لم يبلغوا السادسة عشر من عمرهم، ويعاقب كذلك معد مثل هذه المواقع وكذلك مستوردها[3].

وفي القانون الليبي توجد المادة (409- عقوبات) التي تعاقب على تحريض الصغار دون الثامنة عشرة على الفسق والفجور أو مساعدتهم

---

(1) Guillam Desgens – Pasanau, Au Centre des debat actuels: La protection des mineurs sur l'internet -24/7/2001. disponible enligne en Juillet 2001 a:
http://www.droit-technologie.org/1.2.asp?actuid=1604298204.

انظر القانون رقم 468-98 المؤرخ 1998/6/17 بأن منع والمعاقبة على الجرائم وحماية القصر تعاقب كل من يقوم ببث مواقع دعارة أطفال.

(2) Sur le plan penal, deux infractions contenues dans le Nouveau Code Penal (NCP), ayant pour finalite la protection des mineurs, meritent, concernant le reseau Internet, une attention particuliere. Ainsi: - "le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image d'un mineur lorsque cette image presente un caractre pornographique".

(3) Thibault Verbiest – Pornographique e Internet: comment reprimer? 19 Mai 2001, disponible enligne en juin 2001 a:
http://www.droit-technologie.org/1.2.asp?actu.id=2099182987.

على ذلك أو التمهيد لهم أو القيام بتسهيل ارتكاب مثل هذه الأفعال أو إثارتهم بأية طريقة كانت لارتكاب فعل شهواني أو قام بارتكابه أمامهم. وعلى الرغم من الغموض الكبير الذي يكتنف عبارة (بأية طريقة كانت) الواردة في النص، فإنه مع ذلك يمكن القول بتطبيق هذا النص جزئيا على أفعال الإثارة فقط، إذا كان الطفل على دراية بالجاني، فمثلا لا ينطبق هذا النص على أصحاب المواقع التي تقوم بترويج دعارة أطفال، حال قيامهم ببث عام دون تحديد للمجني عليه، وإنما يلزم أن يكون هناك جان محدد يقوم باستثارة طفل أو أطفال بعينهم. ذلك أن القانون أطلق العنوان للسلوك المادي المستخدم في جريمة إثارة الأطفال وحدها، والذي من الممكن أن يكون باستخدام الإنترنت عن طريق الاتصال بهم أو معهم والقيام بإرسال ملفات جنسية لهم وصور داعرة وحثهم عبر الاتصال المباشر والوسائل السمعية المرئية، التي برع في استخدامها النشء، بالقيام بأفعال جنسية. فمن الممكن هنا أن يقوم المجرم بإسال ملف يتضمن ارتكابه لفعل شهواني لإثارة طفل أو مجموع أطفال، وبقصد حثهم على ارتكاب فسق وفجور، فيقوم الطفل بالإطلاع عليه، ففي هذه الحالة يكون الشخص قد ارتكب جريمة إثارة الأطفال أمامهم كما هي موصوفة في النموذج القانوني للجريمة. وقولنا هذا عائد إلى أن المشرع لم يسع إلى استنطاق الجاني لمظاهر إثارة الطفل بقصد ارتكاب فعل فاسق أو فاجر معه، وإنما معه أو مع غيره، فالجريمة المقصودة هنا في جريمة إثارة الأطفال وليس ارتكاب فعل شهواني معهم، فهذه الأخيرة يحكمها المادتان (407- 408- عقوبات ليبي) في حين مقصود المادة (409- عقوبات ليبي) هي استثارة الأطفال شهوانيا فقط، والمجرم يصل إلى تحقيق هذه النتيجة بأية طريقة كانت ومن ذلك القيام تمكين الطفل من برمجيات

تتعامل مع ملفات تتضمن أفعالا فاسقة أو فاجرة وبحيث يمكن للطفل الإطلاع عليها في أي وقت[1].

على أن هذا النص يحتاج إلى تطوير جزئي في منطق التعامل مع الحركة Action، فممارسة فعل شهواني أمام طفل قد يلصق في ذاكرة الطفل، ويمكن أن يكون مؤشرا على استثارته ودافع إلى ارتكاب أفعال

(1) تنص المادة (409- عقوبات ليبي) على إنه "يعاقب بالحبس كل من حرض صغيرا دون الثامنة عشرة ذكرا كان أو أنثى على الفسق والفجور أو ساعده على ذلك أو مهد أو سهل له ذلك أو أثاره بأية طريقة كانت لارتكاب فعل شهواني أو ارتكبه أمامه سواء على شخص من نفس الجنس أو من الجنس الآخر. وتضاعف العقوبة إذا كان الجاني ممن ورد ذكرهم في المادة (407). كما تنص المادة (407- عقوبات ليبي) على أنه "1- كل من واقع آخر بالقوة أو التهديد أو الخداع يعاقب بالسجن مدة لا تزيد على عشرة سنوات. 2- وتطبق العقوبة ذاتها على من واقع ولو بالرضا صغيرا دون الرابعة عشرة أو شخصا لا يقدر على المقاومة لمرض في العقل أو الجسم، فإذا كان المجني عليه قاصرا أتم الرابعة عشر ولم يتم الثامنة عشر فالعقوبة بالسجن مدة لا تزيد على خمس سنوات. 3- وإذا كان الفاعل من أصول المجني عليه أو من المتولين تربيته أو ملاحظته أو ممن لهم سلطة عليه أو كان خادما عنده أو عند من تقدم ذكره يعاقب بالسجن ما بين خمس سنوات وخمس عشر سنة. 4- وكل من واقع إنسان برضاه يعاقب هو وشريكه بالسجن مدة لا تزيد على خمس سنوات". كما تنص المادة (408- عقوبات ليبي) على أنه "1- كل من هتك عرض إنسان بإتباع أحد الطرق المذكورة في المادة السابقة يعاقب بالسجن مدة لا تزيد على خمس سنوات. 2- وتطبق العقوبة ذاتها إذا ارتكب الفعل ولو بالرضا مع من كانت سنه دون الرابعة عشرة أو شخصا لا يقدر على المقاومة لمرض في العقل أو الجسم، فإذا كانت المجني عليه بين الرابعة عشر والثامنة عشر كانت العقوبة الحبس مدة لا تقل عن سنة. 3- وإذا كان الفاعل أحد الأشخاص المذكورين في الفقرة الأخيرة من المادة السابقة تكون العقوبة مدة لا تجاوز سبع سنين. 4- وكل من هتك عرض إنسان برضاه يعاقب هو وشريكه بالحبس".

شهوانية، ليس بالضرورة مع الجاني ذاته، حيث من الممكن أن الجاني لم يكن يسعى إلى القيام بأفعال شهوانية مع الطفل ذاته، أو يكون قد قبض عليه أو يكون قد أصيب إصابة بالغة في حادث مثلا. ففي هذه الحالة تظل جريمة المادة (409- عقوبات ليبي) قائمة ويلزم تطبيقها على الجاني وإن كان يختلف في شأن طبيعة مدى اعتبار جريمة إرسال ملف أو رسالة إلى طفل صغير، بما يتوافق مع فكرة بأية طريقة كانت لاستثارته شهوانيا، ووجه الاختلاف ينحصر في تحديد طبيعة هذه الجريمة وفيما إذا كانت وقتية أم كانت من الجرائم المستمرة وهو أثر له المنطق التي تستمد منه حركة الزمن في العالم الافتراضي Cyber Time معاييرها وبحيث يحجب عنها مفهوم الحفظ والتسجيل المعتادين، فالاحتفاظ بملف في العالم الافتراضي، كما لو ظل الملف في البريد الإلكتروني للمجني عليه، لا يعني أنه محفوظ بذات الطريقة التي يتم بها الحفظ في القرص الصلب للحاسوب. وعندنا إن الاستمرار قائم بحيث يعد كل مرة يطلع فيها الطفل على الرسالة أو الملف المذكور تجعل حالة الاستمرار قائمة، لأن المشرع لم يتطلب أكثر من مجرد التحريض أو المساعدة سوى التمهيد أو الاستثارة أو أن يكون قد ارتكب أمامه بقصد دفعه إلى ذلك غريزيا دون أن يكون هناك تطلب لتحقق نتيجة محددة وهي قيام الطفل المذكور بارتكاب هذه الأفعال، فيكفي في هذا الشأن ارتكاب النشاط المادي المكون لهذه الأفعال المجرمة.

إن مسألة تحديد القيم الاجتماعية الاقتصادية من الموضوعات التي ينظر إليها في القانون المقارن على أساس كونها تمثل صلب الحدث الرئيسي في إطار تفاعل القانون مع المجتمع في كل دولة. ويهتم المشرع والقضاء في القانون المقارن بالقيم الاجتماعية الاقتصادية لأنها تعد نقطة الارتكاز في الدفاع عن حركة المصالح الاجتماعية الاقتصادية، حيث

يكون تفسير المصلحة على ضوء المفهوم الاجتماعي الاقتصادي للوقائع الإنسانية.

ففي القضاء الأمريكي فإن المبدأ العام الذي يسير عليه هو النظر إلى تحديد المقياس الاجتماعي لتحديد الفعل الفاضح أو الفاحش Obscenity حيث كان القضاء الأمريكي قد وضع معيار الفحش في قضية (Miller v. California, 413 U.S. 15 (1973) بحيث يتم اختبار الفحش وفق البحث في معيار الرجل العادي Average Person وذلك – من ناحية – بتطبيق الضوابط الاجتماعية المعاصرة Contemporary community standards، والتي يمكن بمقتضاها النظر إلى أن العمل ككل يؤدي إلى المتعة الشهوانية Prurient Interest، ومن ناحية أخرى النظر فيما إذا كان النشاط يصور Deplet أو يصف Describe بطريقة عنيفة Patently offensive السلوك الجنسي Sexual conduct كما هو محدد في قانون الولاية. ومن ناحية ثالثة ينظر فيما إذا كان النشاط ككل ينقصه القيم الأدبية والاجتماعية والسياسية والعلمية[1]. والحقيقة إن منطق القيم الاجتماعية يعد عامل ارتكاز حقيقي في تفسير القانون وفق احتياجات المجتمع ككل، ومثل هذا الأمر يقود إلى البحث في القيم الأساسية للمجتمع لبحث درجة الإجرام وتفسير العمل غير المشروع، ومما يؤدي ذلك إلى سلوك مذهب تفسير القانون بحسب المتعارف عليه في المجتمع. ومثل هذا الأمر يقود بالضرورة إلى مسألة المجتمع ذاته في

(1) (1) "The average person applying contemporary community standards' would find that the work, taken as a whole appeals to the prurient interest"; (2) it "depicts or describes, in a patently offensive way, sexual conduct specifically defined by applicable state law"; and (3) "the work, taken as a whole, lacks serious literary, artistic, political, or scientific value". Miller v. California, 413 U.S. Supreme Court.

القانون، وهي مسألة كنا قد تعرضنا لها حين التطرق إلى موضوع المجتمع الذي يلتزم بالدفاع عن حقوقه فيما سلف.

أما القانون الفرنسي فإنه يقرر في تشريعه أهمية جعل الأطفال القصر في موقع مراقبة مستمرة من قبل الأهالي، لاسيما السلطة الأبوية والمنزلية، حيث يشير الفقه القانوني إلى ضرورة قيام القائم بالسلطة الأبوية Titulaires de l'autorite parentale بدور رئيسي في مراقبة القاصر أثناء اتصاله بالإنترنت[1]. وإذا تأملنا القانون الإنجليزي فإننا نجد في القضاء هناك كان له دور كبير في طرح مشكلة تطوير نصوص القانون الذي يتعلق بترويج مواد الدعارة باستخدام الحاسوب والإنترنت[2]، ولقد احتاج الأمر إلى تطوير تشريعين بداية هما قانون الفحش العلني لسنة The protection of Children act 1959. ولقد تم تعديل هذه التشريعات بمقتضى قانون العدالة الجنائية والنظام العام لسنة 1994 The Criminal Justice & Public Order Act 1994 لكي يتلاءم مع لغة عصر المعلوماتية[3].



(1) Guillam Desgnes – Pasanau, op. cit., P.4.

(2) R. v. Fellows & Arnold App. England, 1997, See: Paul Cullen QC – Computer Crime, op. cit., at 213.

(3) Id.

المبحث الخامس
جرائم البث العلني
(النشر - السب والقذف والتشهير - المراسلة)

يعد البث العلني Diffusion en Publique، أحد الخصائص التي تتميز بها تقنية الإنترنت، باعتبارها أكبر حدث علمي بارز منذ اختراع الطباعة. فهي فضلا عن كونها وسيلة حية، وأيضا حيوية، للبث فيها فإنها اجتمعت فيها مظاهر البث السمعي المرئي Audiovisual أيضا، فاحتوت بذلك قوة وسائل وأدوات البث التقليدية (المقروءة - المسموعة - المرئية). فإذا أضفنا إلى ذلك الظاهرة العلنية التي عليها الإنترنت، من حيث كونها إحدى وسائل العلنية كما عرفها قانون العقوبات، إن لم تكن أقواها على الإطلاق، فإن ذلك ليعبر عن القدرة الإيجابية ذات الطابع الفريد للإنترنت. لذلك يمكن عداد الإنترنت وبما تحويه من عالم افتراضي وسيلة يمكنها أن تستوعب حركة البث في كافة مظاهرها.

وعلى الرغم مما سلف فإن نقطة واحدة تظل في منأى عن اتصالها بالإنترنت وهي الالتقاء المادي المباشر بين الأشخاص، وهذه يبنى عليها تفرقة مادية في الحدث يمكن أن يكون لها تأثيرمادي ولكن لا يمتد إلى القانون. والفرض هنا بالطبع إمكانية حدوث اتصال مرئي بين شخصين فأكثر وينطبق على المكان، أما الوصف الخاص وإما الوصف العام للمحل، فمثلا يمكن أن يجتمع عبر الإنترنت عدة أشخاص لكي يتبادلوا أطراف الحديث بالرؤيا المباشرة في ذات الوقت، بحيث يرى أحدهم الآخر أو أنهم جلهم يرون بعضهم ومثال ذلك النظام المؤتمري أو حلقة النقاش News group أو Conference، وفي هذه الحالة تتوافر صفة العمومية إذا كان المؤتمر المذكور مما يسمح بالولوج إليه من قبل أي

كان، فهو في هذه الحالة من الأماكن العامة طالما وجد ما يدل على إمكانية الاشتراك في هذا المؤتمر أو حلقة النقاش حتى بمجرد المتابعة لما يجري، وهو أمر ينطبق عليه مدلول العلنية (1/16- عقوبات ليبي).

ويتخذ البث الفاضح العلني مظاهر عدة إلا أنها تتوحد كلها عبر الإنترنت في كونها بثا، وهو أمر يستفاد منه إن التمييز الحادث بين مظاهر البث هو تمييز حادث في العالم المادي ومصدره القانون، وهو أمر يجد له أثرا عبر الإنترنت أيضا، إذ يميز هناك بين كون البث نشرا، وبين كونه سبا أو قذفا أو تشهيرا، وبين كونه مراسلة بريدية عبر البريد الإلكتروني، وفيما إذا كان هناك علنية أم لا، وفيما إذا كانت العلنية مفترضة في أي من هذه الحالات من عدمه، وذلك لما توفره الإنترنت من مجموعة بدائل تستخدم في التعامل عبرها. على أنه يلاحظ أن المشرع في بعض الأحيان لا يستجيب للعلنية، وبالتالي نجدها غير متطلبة على الرغم من طبيعة الجريمة هنا وكونها من طبيعة الجرائم الفاضحة، والتي تسبب تصغيرا من شأن المجني عليه عند أهل مهنته وبني وطنه. ومع ذلك تتكامل هذه الجريمة ويكون الجاني عرضة للإدانة دون اعتبار لما إذا كان هناك علانية من عدمه، مثل ما هو مقرر في جرائم إهانة الصحفي أو التعدي عليه بسبب عمله، والتي لم يتطلب فيها القانون العلانية. ومن ثم فإنه سواء توافرت العلنية أو لم تتوافر فإن الجريمة قائمة، وهو ما تنص عليه المادة (12) من القانون رقم 96 لسنة 1996 بشأن الصحافة في مصر من أنه "كل من أهان صحفيا أو تعدى عليه – بسبب عمله – يعاقب بالعقوبات المقررة لإهانة الموظف العمومي أو التعدي عليه في (المواد 133-136-1/137) من قانون العقوبات – بحسب الأحوال".

وهنا سوف نتطرق إلى موضوع البث العلني في أشكاله التي تم رصدها فيما سلف، وهي النشر Publication والسب والقذف والتشهير Defamation والمراسلة Mailing وذلك في الفقرات التالية:

أولا: النشر:

ليس المقصود بالنشر هنا هو النشر الصحفي عبر الإنترنت، وإنما مقصوده قيام أي شخص بنشر ما يمكنه أن يقوم به مباشرة تجاه أي شخص، فالنشر المقصود هنا لا يقع في نطاق العمل الصحفي فقط، وإنما بث مباشر على الإنترنت بخطاب مباشر مع الآخرين.

فالنشر عبر الإنترنت ليس هو النشر في العالم المادي، ففي العالم الافتراضي يكون النشر متميزا بخاصية الحرية المطلقة غير المقيدة بإجراءات، سوى تلك التي تتعلق بحجز نطاق اسم Domain Name ثم حجز المساحة اللازمة على الإنترنت لدى أحد مزودي الخدمات، وهذه وتلك متوافرة ويمكن القيام بها بسهولة تامة دون حاجة لكي يكون التأجير من قبل مزود خدمات وطني، بل يمكن القيام بحجز نطاق الاسم والمساحة المرغوبة من مزود دخول في دولة أخرى إن لزم الأمر، والقيام بالبث مباشرة كما لو كان ذلك من مزود دخول بجوار المنزل. فلا يهم فيما إذا كان مزود الدخول في آخر العال أو كان في الشارع الخلفي لمحل إقامة المتهم. ثم يتم بعد ذلك القيام بالبث بأي شكل من الأشكال. فإذا تضمن البث سبا أو قذفا فإن الأمر يتطلب هنا دراسة النصوص للنظر فيما إذا كانت تتناسب مع مثل هذا الحدث أم أنها ليست متناسبة، وهو الأمر الذي يستدعي تدخل المشرع في هذا الشأن. والحقيقة أن النشر عبر الإنترنت إنما هو أقرب إلى البث منه إلى النشر المتعارف عليه في العالم المادي. إذ أن إجراءات النشر عبر الإنترنت لا يتطلب فيها اتخاذ الإجراءات التي يتطلبها القانون للنشر بالمعنى الضيق في العالم المادي،

فمثلا لا يستدعي النشر عبر الإنترنت لزوم اتخاذ إجراءات إيداع المصنف كما هو مقرر في العالم المادي، كما أنه لا يلزم أن يكون النشر محاطا بضمانات النظام العام والآداب...الخ. فمثلا يستطيع أي شخص إنشاء صحيفة عبر الإنترنت، دون لزوم اتخاذ الإجراءات القانونية التي يتطلبها القانون لنشر صحيفة في العالم المادي، وفي هذه الحالة سوف يكون في حل من المساءلة مادامت الصحيفة رقمية. بل أن النشر عبر الإنترنت إنما هو أقرب إلى ممارسة الحرية الكاملة في البث منه إلى النشر، بحيث يخضع الأمر لذوق عضو الإنترنت المطلع على ما يتم نشره. ولذلك آثار في القانون من حيث اقتراب مفهوم النشر عبر الإنترنت من المنطق الواسع له الذي يتخذ شكل البث الكامل بكل حرية. وهذا المفهوم الواسع للنشر عبر الإنترنت يجعل انطباق المدلول الموسع للنشر ي قانون العقوبات متوافقا معه، فمثلا في القانون الليبي فإن النشر غير المشروع يمكن أن يشكل جريمة وفقا للمواد (274-290-291-317-318-319-320- عقوبات ليبي). كما يتولى القانون المؤرخ 1881/7/29 بشأن الصحافة في فرنسا العقاب على البث الإجرامي العلني إذا تم عبر الإنترنت بأسلوب السمعي البصري Audiovisuelle كما لو تم هذا البث عبر أحد حلقات النقاش مثلا Forum de Discussion[1]. ومع ذلك يعتد بالتقادم الصحفي الاستثنائي في حالة

(1) وفي إطار القانون الفرنسي فإنه يلزم الأخذ في الاعتبار بأن القانون المؤرخ 1881/7/29 بشأن حرية الصحافة بعد القانون الأساسي الذي يتشكل معه النظام القانوني للصحافة Le Cadre Legal de la press. وهو القانون الذي تم سنه من قبل مشرع الجمهورية الثالثة، بحيث يمكن القول أنه متوافق مع الإعلان الفرنسي لحقوق الإنسان والمواطن في المادة (11) منه التي تنص على حرية الإنسان في بث أفكاره وآرائه كما له حرية الكلام والكتابة والطباعة شريطة ألا يكون في هذه الحرية

النشر لما يتضمن قذفا عبر الإنترنت، وهو التقادم المقرر في المادة (65) من قانون 29 يوليو 1881[1].

إن البث عبر الإنترنت يتطلب فقط إعداد العدة الخاصة بذلك للقيام به، من حيث اختيار نطاق اسم بحجزه لدى الجهة المختصة، ثم القيام بإعداد موقع[2] لذلك باستخدام تكنولوجيا المعلومات/ الحاسوب والبرمجيات والبيانات تحديدا، ثم استخدام قرص صلب أو مرن أو مضغوط، ممغنط، لكي يتم نقله وإيداعه في الحاسوب الخادم أو الملقم، ثم بعد ذلك استخدام برمجيات أخرى لكي يتم تحميل ذلك على الإنترنت، وذلك يتم بطريق الحيازة المشروعة لمساحة في مضيف، مع ضرورة حيازة برمجيات أخرى[3] يمكن بطريقها القيام بإنزال هذا الموقع عند الحاجة للإجراء تعديل ما في هذا الموقع. ويترتب على هذا الاختلاف المادي بي البث عبر الإنترنت وبين النشر في العالم المادي أثر قانوني هام يتعلق بتطبيق التقادم على نوعية الجرائم التي ترتكب عبر بث الإنترنت، مثلما هو الحال فيما يتعلق بتطبيق المادة (65) من قانون

=

تعسفا من أي نوع. ولقد تم تعديل القانون المذكور بمقتضى القانون المؤرخ 1982/7/29 بشأن الاتصالات السمعية المرئية ثم بمقتضى القانون المؤرخ 1986/8/1 بشأن هيئة النظام القانوني للصحافة ثم أضيف إلى هذه النصوص القانون المؤرخ 1990/7/13 بشأن العنصرية، وهو القانون المعروف باسم تشريع Loi Gayssot.

(1) Cass. Cr. 30/1/2001, No.655, Disponible enligne en Oct. 2001 a : http://www.juriscom.net

(2) Stephane Liti – Le Changement d'adresse sans demenagement, Nouvelle cause dirresponsabilite penale, commentaire du jugement rendo par la 17eme ch. Corr. Du TGI de Paris, le 28 Jan. 1999, disponible en ligne a : http://www.legalis.nt/inet/commentaires/lilti-280199.htm

(3) Uploader – Downloader.

الصحافة الفرنسي. إذ أن التقادم بثلاثة أشهر المقرر في هذا القانون يسري من تاريخ النشر المادي لموضوع الجريمة في حين أن التقادم لا يسري على جرائم البث عبر الإنترنت، وإن كان هناك رأي يذهب إلى القول بأن التقادم يسري كما هو الحال في جرائم النشر المادي، إلا أنه يتجدد كلما كان هناك تغييرا للخادم المضيف الذي وضع فيه الموقع الذي يحتوي على جرائم البث، قبل وذهب هذا الرأي إلى التأكيد على أن مجرد تغيير نطاق الاسم Domain Name يؤدي بالضرورة إلى تحديد التقادم المشار إليه[1].

ثانيا: السب والتشهير:

تعد هذه الجرائم من أقدم الجرائم المرتكبة عبر الإنترنت، وذلك لما يتمتع به عضو الإنترنت دائما - وبحسب المعتقد السائد - من حرية كاملة عبر الإنترنت، لذلك يجب ألا نستغرب إذا كنا قد ارتكبنا أيا من الأفعال المشار إليها عبر الإنترنت في المساء، لنجد في صباح اليوم التالي دعوى تباشر ضدنا في أحد المحاكم وإعلانا بالحضور لسماع الحكم علينا لأنه في يوم....الخ.

(أ) السب: وهو خدش شرف شخص أو اعتباره في حضوره، وذلك بتوجيه كلمات مقذعة في مواجهة شخص أو أشخاص معينين بدقة كافية[2]، على أن يكون حاضرا كل من الجاني والمجني عليه الواقعة، ويشمل السب والقذف نسبة وقائع معينة لكي يصل إلى مجرد توجيه عبارات تعد خدشا للشرف والاعتبار دون أن يكون فيه إسناد لواقعة

(1) Stephane Lilti, op. cit.

(2) طعن جنائي مصري رقم 20471 لسنة 60ق جلسة 1999/11/14. المحامي/ مصر ع. 1 لسنة 2001، ص206.

معينة كما هو الشأن فيما هو مقرر في المادة (306- عقوبات مصري)[1]. وإن كانت بعض التشريعات تتطلب أن تكون الواقعة علنية. وذلك مثلما هو الحال فيما تقضي به المادة (R-624-4) من قانون العقوبات الفرنسي الجديد التي تنص على أنه "السب غير العلني الواقع في مواجهة شخص أو مجموعة أشخاص بسبب الأصل أو الانتماء أو عدم الانتماء، حقيقة أو مفترضا، على عرض أو أمة أو عنصر أو دين محدد، معاقب عليه بالغرامة المقررة على الجنحة من المستوى الرابع"[2].

أما القانون المؤرخ 1881/7/29 بشأن حرية الصحافة فإنه يعرف السب بأنه "كل تعبير مهين أو شائن، أو مصطلحات احتقار أو قدح التي لا تؤدي إلى الاتهام بأي فعل"[3].

وكانت المادة (308 مكرر – عقوبات مصري) التي تنص على أنه "كل من قذف غيره بطريق التليفون يعاقب بالعقوبات المنصوص عليها في المادة 303. وكل من وجه إلى غيره بالطريق المشار إليه بالفقرة السابقة سبا لا يشتمل على إسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشا للشرف أو الاعتبار يعاقب بالعقوبة المنصوص عليها في المادة 306. وإذا تضمن العيب أو القذف أو السب الذي ارتكب بالطريق

(1) طعن جنائي مصري رقم 12952 لسنة 60ق جلسة 2000/2/22. المحامي/ مصر ع. 1 لسنة 2001، ص206.

(2) Art (R-624-4-CPN Fr.) « L'injure non puplique commise envers une personne ou un groupe de personnes a raison de leur origine ou de leur appartenance, vraie ou supposee, a une ethnic, une nation, une race ou une religion determince est punie de l'amende prevue pour les contraventions de la de classe ».

(3) L'article 29 de la loi du 29 Juillet 1881 definit l'injuire comme « toute expression outrageante termes de mepris ou invective qui ne renferme l'imputation d'aucun fait ».

المبين بالفقرتين السابقتين طعنا في عرض الأفراد وخدشا لسمعة العائلات يعاقب بالعقوبة المنصوص عليها في المادة 308"[1].

على أن المشرع قد يتوسع في مسألة الحضور المادي للمجني عليه، بحيث يكون السب متوافرا إذا لم يكن المجني عليه حاضرا ماديا بشخصه، مثلما هو الحال فيما تقضي به المادة (306- عقوبات مصري) من أن "كل سب لا يشتمل على إسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشا للشرف أو الاعتبار يعاقب عليه في الأحوال المبينة بالمادة 171 بالحبس مدة لا تتجاوز سنة وبغرامة لا تقل عن ألف جنيه ولا تزيد على خمسة آلاف جنيه أو بإحدى هاتين العقوبتين".

المادة (438- عقوبات ليبي) التي تنص على أنه "كل من خدش شرف شخص أو اعتباره في حضوره يعاقب بالحبس مدة لا تجاوز ستة أشهر أو بغرامة لا تجاوز خمسة وعشرين دينارا. وتطبق العقوبات ذاتها على من ارتكب الفعل بالبرق أو التليفون أو المحررات أو الرسوم الموجهة للشخص المعتدى عليه. وتكون العقوبة الحبس لمدة لا تجاوز السنة أو الغرامة التي تجاوز أربعين دينارا إذا وقع الاعتداء بإسناد واقعة معينة".

وفي قانون العقوبات الإيطالي تعاقب المواد (594-595) على السب. كما تضمن القانون الأمريكي نصا هو (Sec. 223 a 47) يعاقب على استخدام عبارات قذرة إذا كان الغرض منها مضايقة Annoy الغير[2].

(1) انظر في ذلك: د. جميل عبد الباقي الصغير، الأحكام الموضوعية، المرجع السابق، ص29.

(2) USA v. William M. Landham, 2001 FED App. 01 75P (6th Cir.), No. 99-5471, May 25, 2001.

(ب) التشهير: والتشهير Libel من جرائم البث المباشر في القانون، وهو في كل الأحوال نوع من القذف، وإن كان يستلزم في القانون الأمريكي أن يكون كتابة. في حين أن التشهير بالكلام يطلق عليه في المصطلح الأنجلوفوني Slander. فالأساس الذي يعتمد عليه التشريع الأمريكي في إطار التشهير ينطلق من تهديد سمعة شخص ما Man's Reputation التي تمثل المصلحة التي يحميها القانون هنا. حيث يؤدي التشهير إلى التقليل من قدر الشخص في نظر المجتمع والناس أيا كانوا، مثل أقاربه وجيرانه والأشخاص الذين لهم علاقة بهم أيا كانت نوعية هذه العلاقة، كما لو كانت هذه العلاقة عائلية أو شخصية أو تجارية أو مالية...الخ.

وهو ذات الأمر في القانون الفرنسي فالمادة (R. 624-3) من قانون العقوبات الفرنسي الجديد تنص على أنه "القذف غير العلني يقع في مواجهة شخص أو مجموعة أشخاص بسبب أصلهم أو انتمائهم أو عدم انتمائهم، الحقيقي أو المفترض، إلى عرق أو أمة أو جذر أو دين"[1]. كما تنص المادة (439- عقوبات ليبي) على أن يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة لا تجاوز خمسين دينارا كل من اعتدى على سمعة أحد بالتشهير به في غير حضوره لدى عدة أشخاص، وذلك في الأحوال المنصوص عليها في المادة السابقة. وإذا وقع التشهير بإسناد واقعة معينة تكون العقوبة الحبس الذي لا تتجاوز مدته السنتين أو الغرامة التي لا تجاوز السبعين دينارا. وإذا حصل التشهير عن طريق الصحف أو غيرها

(1) La diffamation non puplique commise envers une personne ou un groupe de personnes a raison de leur origine ou de leur appartenance ou de leur non-appartenance, vrai ou supposee, a une ethnie, une nation, une race ou une religion determinee est punie de l'amende prevue pour les contravention de le 4e classe ».

من طرق العلانية أو في وثيقة عمومية تكون العقوبة الحبس الذي لا يقل عن ستة أشهر أو الغرامة التي تتراوح بين عشرين دينارا ومائة دينار. وإذا وجه التشهير إلى هيئة سياسية أو إدارية أو قضائية أو إلى من يمثلها أو إلى هيئة منعقدة انعقادا صحيحا لتزاد العقوبة بمقدار لا يجاوز الثلث".

ثالثا: السب عبر الإنترنت

إذا كان الفقه والقضاء قد وجد صعوبات حال البحث عن معيار يمكن بمقتضاه التمييز بين ما هو مقرر في التشريع من تمييز بين الطريقة التي يمكن بها ارتكاب السب والقذف[1]، فإن الأمر استقر فيما يبدو على المعيار الاحتياطي الدائم، وهو معيار واقعي مستمد من البحث في كل حالة على حده، وذلك لصعوبة التمييز بين السب والتشهير في الحالة الواقعية التي يكون فيها الفرد قائما وحاضرا أمام الجاني.

أما في الحالة الاعتبارية فإن المشرع كثيرا ما يقوم بتحديد حالات يكون فيها المجني عليه غير حاضر واقعة السب حضورا ماديا كاملا وإنما جزئيا بحيث يستشعر أحد أعضاء المجني عليه واقعة السب كما هو الشأن في سماعة ورؤية واقعة السب عبر الاتصال الهاتفي والهاتف المرئي أو البرقي أو الكتابة في محرر أو إعداد رسوم ما، في حين إن التشهير يلزمه، فضلا عن عدم وجود الشخص أو حضوره الواقعة، أن ترتكب أمام عدة أشخاص، كما يمكن أن ترتكب في الصحف أو غيرها من طرق العلانية أو في وثيقة عمومية، إذ كل ما يتطلبه المشرع في واقعة التشهير ألا يكون المجني عليه حاضرا. أما إذا كان الشخص حاضرا فإن الواقعة في هذه الحالة تكون سبا وليست تشهيرا.

(1) David Loundy - Computer information systems Law & system Operator Liabilty, the Seattle Uni. Law Review, Vol. 21, No.4, Summer 1998, P.16.

لذلك فإن النطاق المادي لبحث مدى توافر واقعة السب وتمييزها عن التشهير يستلزم الحضور المادي كليا أو جزئيا لواقعة الجريمة، حتى يمكن القول بأن الواقعة تكون جريمة سب أو جريمة تشهير. ففي واقعة السب والقذف فإن الركن المادي يتم بناؤه على أساس تحديد شخص المجني عليه وتعيينه التعيين الكافي لا محل معه للشك في معرفة شخصيته[1]. على أن الأمر هنا ليس بهذه السهولة عبر الإنترنت، ذلك إنه لما كان من الصعوبة، إن لم يكن من المستحيل، توافر الحضور الكلي للمتهم والمجني عليه حتى يمكن القول بوجود سب ما، فإن المسألة يمكن أن تكون محل جدل فيما يتعلق بارتكاب السب الجزئي. ذلك إنه يختلف الحال حول هذه المسألة فيما إذا كان المجني عليه حاضرا على الإنترنت وفي حالة اتصال مباشر مع الجاني، كما لو كان الاثنان معا في إحدى حلقات الناقش، وما إذا كان الاتصال مباشرا بينهما أم إن الجاني يتحدث مع آخرين دون حضور للمجني عليه (تشهير) أم بحضور المجني عليه (سبا) حسب الأحوال.

ومما يدخل في إطار التشهير قيام الجاني ولو باستخدام الاستعارة ببث رسالة باستخدام حلقات الناقش[2] وكذلك عبر قوائم المراسلة Mailing List التي تذخر بها المواقع عبر الإنترنت للتعبير عن الرأي أو الفكرة وكذلك البريد الإلكتروني[3] إلى عدد غير محدود، وفي هذه الحالة يستفيد المجني عليه من الاحتمال إذا وصلته نسخة من هذه

(1) طعن جنائي مصري رقم 20471 لسنة 60 ق جلسة 1999/11/14 (المحامي - صر العدد 1 لسنة 2001، ص209).

(2) Guillame Desgens – Pasanau – Du Bon Usage d'un Forum de discussion, P.3- disponble en ligne en 13 Mars 2001 a : http://www.droit-technologiw.org.

(3) David Loundy, op. cit., at 17.

الرسالة. أما إذا لم تصله فإن الأمر يظل في إطار التشهير كقاعدة، وفي هذه الحالة فإن المثار هنا هو موضوع العلانية التي نرى توافرها عبر الإنترنت، إذ كل ما يتطلبه المشرع في التشهير أن تكون واقعته قد تمت لدى عدة أشخاص، دون استلزام لما إذا كان حضورهم المادي متطلبا أم لا، وهو غير الأمر فيما يتعلق بالمحررات حيث يلزم أن يعترف المشرع بالوجود الرقمي لهذه المحررات. وتعد حلقات النقاش والقوائم البريدية أو التراسلية مجالا حيويا لتطبيق قانون النشر الصحفي على وقائع التشهير عبر الإنترنت في فرنسا بمقتضى القانون المؤرخ 1881/7/29 بشأن الصحافة المعدل بالقانون المؤرخ 1986. فالقانون الأخير يميز بين القذف وبين الإساءة بالسب وفقا للمادة (29) منه، حيث تعرف المادة الأخيرة القذف بأنه كل ادعاء أو اتهام بفعل يجلب عدوان على سمعة أو اعتبار لشخص ما أو لمجموعة ينسب إليها الفعل"[1]. على أن السؤال الأكثر إثارة للجدل يتعلق بموضوع مضمون الرسالة التي يمكن أن تكون مجرمة بمقتضى التشريعات المختلفة في هذا الإطار.

رابعا: تكوين المراسلة الإلكترونية مجرمة

يعد نظام التراسل فحوى الاتصال بالإنترنت، وإذا كانت التطورات المعاصرة في تكنولوجيا المعلومات قد وصلت إلى حدود الاتصال الفوري بالصوت والصورة، بحيث يجعل الإنسان في حركة اتصالية مباشرة مع الغير، دون اعتبار لما إذا كان هناك حاجز مادي من أي نوع، فإن مثل هذا الأمر بالطبع لن يترتب عليه تراجع من أي نوع أيضا لنظام التراسل

(1) L'article 29 de la Loi du 29 juillet 1881 definit la diffamation comme « toute allegation ou imputation d'un fait qui porte atteinte a l'honneur ou a la consideration de la personne ou du corps auguel le fait est impute ».

عبر الإنترنت. ولذلك عدة أسباب أبرزها على الإطلاق مسألة الاعتراف القانوني بموضوع الرسالة الإلكترونية تحديدا حيث أخذت الرسالة الإلكترونية حظها القانوني ووصلت إلى مستوى الرسمية في هذا الإطار. بحيث يمكن تقديمها كدليل أمام المحاكم وذلك كنتيجة طبيعية للاعتراف القانوني المذكور بمخرجات الحاسوب.

والمراسلة الإلكترونية يتسع مدلولها لأبعد من الرسالة التي تبث عبر الإنترنت في صيغة رسالة عبر نظام البريد الإلكتروني. إذ يتسع مدلولها ليصل إلى قائمة التراسل أو ما يطلق عليها في المصطلح الإنجليزي Mailing List، وهو نظام تراسلي جماعي يمنح صلاحية بث رسالة إلى مجموعة من الأشخاص، قد تجمعهم أفكار مشتركة حول موضوع ما أو موضوعات متعددة، قاموا بتسجيل بريدهم الإلكتروني مسبقا في هذه القائمة، بقصد تناول هذا أو ذاك الموضوع، فيقوم هذا النظام ببث هذه الأفكار التي أرسلها هذا أو ذاك العضو في هذه القائمة لكل من يشترك فيها من أشخاص دون حاجة لأن يكون على دراية بهم أو بشخصياتهم. وغني عن البيان أن مثل هذا النظام التراسلي كان قد نشأ في ظل أفكار العمل الجماعي، بحيث يتم تداول الأفكار في إطار المنظمة الواحدة حول موضوع ما، فهو في الحقيقة نظام مشجع للعمل الجماعي، حال تطلب وجود أكثر من رأي فيما يخص أحد الموضوعات.

ومما يندرج في إطار التراسل الإلكتروني أيضا، كأثر لاتساع مدلوله عما هو عليه الحال في العالم المادي، ما يسمى بنظام حلقات النقاش Newsgroups، وهي تتناول في موضوعها جلسة لمناقشة موضوع أو موضوعات فورية، أو حديث الساعة. وقد تكون في إطار مجموعة على معرفة بأحدهم الآخر، بحيث يكون دور الدخيل مجرد دور استفهامي، وبحيث يترك سؤالا فقط لأحد المناقشين دون أن يتدخل في موضوع

المناقشة حيث يكون ذلك غير مسموح به، أو أن يسمح في مثل هذه المجموعات للغير بالدخول في حلقة النقاش فيطرح أفكاره علنا على مجموعة النقاش هذه، كما لو كان الأمر مباحا للجميع في المشاركة. والواقع أمام تعدد أنواع وبدائل النظام التراسلي عبر العالم الرقمي، فإن الأمر يبرز كما لو كان هناك نوع من الخلط، وبحيث يطغى هذا الخلط على تحديد التكييف المناسب للعدوان في هذا الإطار، وفيما إذا كان الأمر ينطبق عليه مفهوم الرسالة كما هي معرفة في العالم المادي أم أن لها مفهوما آخرا موسعا، وبحيث يكون مدلوله متوافقا مع الصورة التي يمكن استخدامها بها في العالم الرقمي.

ومما يؤخذ في الاعتبار هنا إن القانون الجنائي المقارن يأخذ في الاعتبار الكيفية التي يتم بها التراسل ماديا، دون أهمية لعامل الوقت، وبحيث يعد زمن الاتصال يبدو كما لو لم يكن له قيمة في هذا الشأن. إذ عديدة هي النصوص التي تشتبه على الكتابة، مثل الإبراق والفاكس والاتصالات الهاتفية، ومن ذلك ما هو مقرر في تشريع ولاية أركانساس الأمريكية ARK CODE ANN. 5-41-108 (2000) الذي يعترف بارتكاب جريمة التخويف أو الترهيب أو التهديد أو الإساءة ضد أي شخص باستخدام البريد الإلكتروني أو أية وسيلة اتصال أخرى، أو أني قوم الشخص بارتكاب جريمة بالمراسلة حال إرسال رسائل دعاية مثيرة وغير منظمة Unsolicited bulk email باستخدام شخصية وهمية Forged identity، مثلما هو الحال في تشريع Illinois الذي يعاقب على تزييف أو تزوير Falsifies or forges التحويل المعلوماتي بطريق الرسالة الإلكترونية بأية مضمون، حال كون موضوع هذا التراسل بريد تافه عبر الإنترنت غير معروف مصدره.

وعليه يتسع مدلول الرسالة المجرمة عبر الإنترنت لكي تشمل في محتواها ليس فقط جرائم الأخلاق، وإنما أيضا جرائم أخرى تتخذ الطابع التقليدي، كما هو الشأن في جرائم التهديد بالقتل أو بارتكاب جريمة ضد النفس والمال. كما يتسع أيضا مدلولها في إطار الجريمة التقنية بحيث تتخذ أبعادا تقنية محضة، كما هو الشأن في تخريب قواعد البيانات أو هدم نظام المعلومات باستخدام الرسائل الإعلانية مجهولة المصدر. ولعل أشهر قضية تهديد هي تلك التي قام بها Christopher James Reincke (18 عاما) طالب في جامعة Illinois بالولايات المتحدة الأمريكية، حيث قام في 2001/12/4 بإرسال رسالة عبر البريد الإلكتروني إلى الرئيس كلينتون وقام بتهديده فيها بالقتل.

وفيما يتعلق بطبيعة العبارات التي استخدمت في السب والقذف، فإنه لا يختلف حالها عما هو عليه الحال في العالم المادي، إذ تستخدم ذات العبارات التي يتم استخدامها في العالم المادي في جرائم السب والقذف والتشهير عبر الإنترنت. ولا يقدح هنا في عملية التغاير والاختلاف الاجتماعي والثقافي بين الشعوب للقول بعدم إمكانية تحديد مفهوم العبارات المستخدمة. ذلك أن تحديد مرامي العبارات وتحري مطابقة الألفاظ للمعنى الذي انتهى إليه الحكم وتسميتها باسمها المعين في القانون وتحديد ما إذا كانت سبا أم قذفا أم عيبا أم إهانة أم تشهيرا هو من مسائل القانون التي يخضع فيه ما ينتهي إليه قاضي الموضوع لرقابة محكمة النقض[1]. ومثل هذا الأمر يتوافق مع وسيلة إثبات القصد الجنائي في هذه الجرائم، حيث يلزم لإثباته والتحقق من قيامه أن تكون الألفاظ المستخدمة

(1) طعن جنائي مصري رقم 3087 لسنة 62ق، جلسة 2000/5/8 (المحاماة/ مصر العدد 1 لسنة 2001، ص207).

في السب والقذف والتشهير شائنة بذاتها[1]، وتبتعد عن مدلول مجرد النقد المباح الذي لا يتضمن المساس بشخص صاحب الأمر أو التشهير به أو الخط من كرامته[2]. إذ يصلح أن يكون مبنى التجريم هنا أن يكون ذلك باستخدام نطاق اسم يحتوي على عبارات غير أخلاقية، مثل Fuckmickey.multimania.com حتى أن تضمن الموقع مجموعة صور لأفراد برزت فقط وجوههم[3].



(1) طعن جنائي مصري رقم 4933 لسنة 62ق، جلسة 2000/5/15 (المحاماة/ مصر العدد 1 لسنة 2001، ص207).
(2) طعن جنائي مصري رقم 3087 لسنة 62ق، السابق.
(3) TGI Meaux, 3eme Ch, Correc. 19/11/2001 (Ste Eurodisney S. C. A. & autres c/ A. A.) http://www.juriscom.net.

المبحث السادس
المطاردة والإزعـاج

المطاردة عبر الإنترنت Cyberstalking تعني قيام عضو الإنترنت بمراسلة واتصال مستمر بعضو أو أعضاء آخرين بقصد إزعاجهم Harassing وتهديدهم Threatening ومضايقتهم وإقلاق راحتهم. ويعد العنصر النسائي عبر الإنترنت الهدف الأكثر تفاعلا مع جريمة المطاردة والإزعاج هنا. إلا أن ذلك لا يمنع من وجود صور وأشكال أخرى للمطاردة، كما هو الشأن في مطاردة الموظف العام[1]، وكذلك مطاردة الأطفال بث الأفكار المعادية للأجانب من عنصرية وكراهية إلى غير ذلك من مظاهر وأشكال هذه الجريمة. ومن ذلك أيضا ما هو مقرر من مظهر تقليدي لجريمة المطاردة حسبما هو مقرر في المادة (472- عقوبات ليبي) التي تنص على أن "كل من تسبب في مضايقة الغير أو إقلاقهم في محل عام أو مفتوح أو معروض للجمهور أو ضايقهم أو أقلقهم باستعمال التليفون أو استعمله لأي سبب ذميم آخر يعاقب بالحبس مدة لا تجاوز شهرين أو بغرامة لا تجاوز عشرين دينار".

وإذا كانت الإنترنت تعتمد على حركة الاتصالات عموما، وكانت في مرحلة زمنية تعتمد على خطوط الهاتف العادية، فإنه مع ذلك لا يمكن القول بامتداد مثل هذا النص للانطباق على الجرائم المرتكبة عبرها، لكون الإنترنت ليست هي الهاتف تحديدا كما هو مقرر في النص المذكور، بالإضافة إلى كون الإنترنت تقنية تعتمد المعلوماتية، فهي هجين ناتج عن مزج هذا وذاك.

(1) Paul Cullen QC – Computer Crime, op. cit. at 217.

أولا: جريمة المطاردة في التشريع المقارن

في القانون الولائي الأمريكي يوجد حوالي ستة عشرة ولاية قامت بسن تشريعات لمكافحة المطاردة عبر الإنترنت، ويكتفي بعض هذه التشريعات بوجود أي شكل من أشكال المطاردة، في حين يتطلب بعض هذه التشريعات قيام مرتكب الجريمة بإرسال تهديد حقيقي Transmit a credible threat للضحية أو عائلته أو أي شخص. وبعض الولايات الأخرى قامت بعد نطاق نصوص الاتصالات الهاتفية الفاحشة Obscene phone call بحيث تشمل عبارة Electronic communication device للاتصال بشخص وتهديده بارتكاب ضرر به أو بعائلته، مثل ولاية كاليفورنيا الأمريكية التي تعد من أوائل الولايات (الدول) التي قامت بسن تشريع يعاقب على ارتكاب جريمة المطاردة Cal. Penal code sec. 646. 9، وتلاها سبع ولايات هي Alaska – Connecticut – Delaware – Michigan – Montana – Oklahoma & Wyoming. ومن التشريعات الولائية الحديثة التي تأخذ بتقرير جريمة المطاردة عبر الإنترنت تشريع ولاية أركنساس الأمريكية التي تجرم قيام أي شخص بغرض التخويف أو التهديد أو الإساءة بالقيام بمطاردة أي شخص باستخدام المراسلة أو البريد الإلكتروني أو أية وسائل اتصالية حاسوبية، وتتضمن هذه المراسلات التهديد بارتكاب أضرار مادية أو عدوان على الملكية أو كانت تحتوي هذه المراسلات على أسلوب فاحش أو فاسق أو لغة مدنسة.

ويعاقب التشريع الفيدرالي الأمريكي على المطاردة عبر الإنترنت، فقد أدين Jack Backe، وهو طالب جامعي، بمقتضى نص القسم © US Code Tit. 18 Sec. 875، كونه في تاريخ سابق استخدم البريد الإلكتروني والمجموعة الإخبارية لبث قصة خطف وقتل شخص ما،

ويلزم المحكمة وفق النص السالف أن يثبت لديها ثلاثة عناصر أساسية حتى يمكن الجزم بوقوع الجريمة وهي القيام بالتداول Transmission بين الولايات وأن يكون هناك اتصال يتضمن التهديد وأن يكون التهديد بقصد إحداث ضرر أو خطف لشخص آخر. كما يعاقب التشريع الفيدرالي الأمريكي على مطاردة الرئيس الأمريكي إذا اقترنت هذه المطاردة بتهديد ما US Code Tit. 18 Sec. 871 بأية وسيلة اتصال مكتوبة أو مقروءة أو مسموعة ورقية أو مطبوعة أو رسالة أو وثيقة مادامت تحمل في مضمونها تهديدا ما، وإن كان يشترط في جريمة مطاردة الرئيس الأمريكي أن تكون أحد أفعال المطاردة كالتهديد أو غيره ذات خصوصية صادرة عن الجاني وموجهة إلى الرئيس الأمريكي دون تلك الإشارات العامة.

وتعد جريمة التهديد من أشهر جرائم المطاردة عموما، والتهديد من الجرائم الشكلية التي لا يستلزم فيها حدوث نتيجة محددة، إذ يكفي فيها مجرد ارتكاب النشاط المادي تحديدا، وليس الركن المادي كلية، وفي هذه الحالة يقوم التهديد كجريمة ويستحق مرتكبها العقاب. ويعاقب القانون الولائي الأمريكي على التهديد كجريمة شكلية، فإكراه شخص على التواجد في المنزل، يعد من جرائم التهديد. كما أن القيام بتهديد شخص باستخدام رموز توحي بأن عدوانا محتمل الحدوث ضده يعد جريمة تهديد، كما لو قرر شخص أنه ينتمي إلى P.D.L. حال وجود خاصم فوري مع آخر، فإن هذا يشكل جريمة تهديد، دون لزوم معرفة طبيعة مثل هذه الكلمات، وما تعني كمختصرات، طالما أن الواقعة اتفقت مع الخصومة القائمة، مادام قد ترتب على الواقعة إدخال الرعب والخشية من وقوع جريمة على المجني عليه.

أما في القانون الإنجليزي، فيعد قانون الاتصالات لسنة 1984 هو القانون الذي يحكم واقعة المطاردة، حيث يعاقب القسم (43) منه على استخدام نظام اتصال عمومي A public telecommunications system لإرسال تهديد Threat أو مواد فحش Obscene أو مضرة Offensive، ويستشعر البعض من الفقه الإنجليزي كفاية هذا النص لانطباقه على البيانات Data التي ترسل عبر الإنترنت. وإن كان يرى أن في قانون الحماية ضد الإزعاج لسنة 1997 ما يكمل القانون الأول المشار إليه.

ثانيا: تحديد نشاط المطاردة

إن مصطلح المطاردة الجديدة التي لم يكن القانون الأنجلوفوني يعترف بها، ولقد كان السبب الرئيسي في بروز هذا المصطلح هو التحرش الذي يصل في أغلب الأحيان إلى ارتكاب جرائم. والمصدر الأساسي لإقرار هذا النوع من العدوان هو موضوع المعاكسات التي يتعرض لها المجني عليه في هذه الجريمة. والواقع أن سلوك المطاردة يحمل على مفهوم القيام بمجموعة أفعال Course of Conduct[1] أو أنشطة تقوم على أساس فكرة الخوف من أفعال تجعل المجني عليه يعتقد اعتقادا جازما بأنه عرضة لنتائج إجرامية من نوع ما. فهي تحمل على مفهوم التهديد، كما تحمل أيضا على مفهوم الترهيب. دون اعتداد هنا بنية الجاني وفيما إذا كان يهدف بعمله هذا إلى القيام بما هو مشروع. وسلوك المطاردة عبر الإنترنت يجد له متسعا، إذ يمكن باستخدام البريد الإلكتروني القيام بمراسلة شخص ما، واستمرار مراسلته بهدف تخويفه أو تهديده. ويجب أن يرتكب الجاني فعل المطاردة مرتين على الأقل لكي

(1) Sec. 4 of the 1997 act (England).

يمكن القول بتوافر الركن المادي كاملا في هذه الجريمة[1]، وذلك ما يجعل هذه الجريمة تختلف عن التهديد الذي يحمل على كفاية ارتكاب التهديد ولو لمرة واحدة. وعليه فقيام عضو الإنترنت بمطاردة شخص آخر في حلقات النقاش بما يترتب على هذا النشاط تسبيب إزعاجا وخوفا في نفس المجني عليه هنا، يمكن أن يكون مثل هذا النشاط مرتبا لجريمة مطاردة.

والحقيقة أن في مثل هذه الجريمة، ذات الطابع الجديد، يمكن القول بوجود جذور لها في القانون الليبي، كما هو الحال في المادة (359- عقوبات ليبي) حيث جاء في هذه المادة نشاط التتبع الذي يحمل بالتأكيد على مفهوم المطاردة حيث اعتبر المشرع الليبي هذا التتبع من التدابير غير المشروعة[2]. وإن كان يحتاج مثل هذا النص الأخير إلى مواءمته مع تكنولوجيا المعلومات، إذ يكفي مصطلح التتبع هنا بشرط الاستمرار لكي يفي جريمة المطاردة حقها في القانون.

(1) Paul Cullen QC. Op. cit.

(2) تنص المادة (359- عقوبات ليبي) على أنه "يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تقل عن مائة دينار ولا تجاوز خمسمائة دينار أو بإحدى هاتين العقوبتين، كل من استعمل القوة أو العنف أو الإرهاب أو التهديد أو التدابير غير المشروعة، بقصد إرغام الغير على الامتناع عن العمل أو إرغام رب العمل على استخدام شخص ما أو منعه من ذلك. وتطبق العقوبة ذاتها إذا كان القصد منع أي شخص من الاشتراك بأية نقابة. ويطبق حكم هذه المادة وإن استعملت القوة أو العنف أو الإرهاب أو التدابير غير المشروعة مع زوج الشخص أو مع أولاده. وتعد من التدابير غير المشروعة الأفعال الآتية على الأخص: أولا: منع الشخص المقصود من مزاولة عمله بإخفاء أدواته أو ملابسه أو أي شيء آخر مما يستعمله أو بأية طريقة أخرى. ثانيا: تتبعه بطريقة مستمرة في غدوه ورواحه. ثالثا: الوقوف موقف التهديد بالقرب من منزله أو بالقرب من أي مكان يقطنه أو يشتغل فيه.

وما يترتب عليه من نشاط المطاردة يجب أن ينعكس في نفس المجني عليه بالضرورة، دون أهمية لما إذا كان الجاني Stalker في العالم المادي أو الافتراضي CyberStalcker قد يرتكب جريمة ضد المجني عليه، فهذا الأخير يسمى مجنيا عليه في القانون بمجرد تكرار ارتكاب المطاردة لمرتين فأكثر ولو على فترات مختلفة، فقد يقوم الجاني بمطاردة فتاة في حلقة نقاش أو بطرقة المراسلة الإلكترونية، ثم يقف نشاطه لبضعة أيام ثم بعد ذلك يكرر محاولته معها مرة أخرى، فهنا يتوافر نشاط المطاردة، ويتحقق الركن المادي في الجريمة.

ولا يشترط القانون نشاط موحد للمطاردة، إذ يمكن أن تقع هذه الجريمة باستخدام سلوك واحد بشكل مكرر، كما هو الشأن في التتبع المستمر المقرر في القانون الليبي، أو أن يقع بأكثر من شكل، كما لو قام الجاني بمطاردة شخص آخر في حلقة نقاش ثم بعد ذلك يتولى مطاردته باستخدام البريد الإلكتروني أو بمراسلته عبر قاعدة بيانات سجل الزيارات في الصفحة الخاصة به على موقعه عبر الإنترنت. كذلك لا يشترط أن يكون المظهر الإجرامي ظاهرا في سلوك الجاني، بل يكفي – في رأينا – أن يكون مسلك الجاني ليس به نوايا إجرامية، فأسلوب الحث على استمرار الحديث عبر حلقة نقاش مع شخص محدد ربما يكون ظاهرا منه حسن النية، ومع ذلك يكفي مجرد القيام بهذا النشاط للقول بتوافر الجريمة. ففي مثل هذه الحالة يكفي أن يكون المجني عليه غير مطمئن لاستمرار هذا الشخص في النقاش معه. فإذا استمر الجاني في تتبع المجني عليه من غرفة إلى أخرى ففي هذه الحالة تتوافر المطاردة، شريطة أن يكون المجني عليه قد أعلن له صراحة أو ضمنا ممانعته في استمرار النقاش معه، أو مطالبته عبر البريد الإلكتروني بالكف عن مراسلته.

ويكفي للقول بتوافر الممانعة الضمنية ألا يقوم المجني عليه بالرد على مراسلات الجاني في الوقت الذي يستمر فيه الجاني في المراسلة مطالبا المجني عليه بالرد أو بإيجاب طلباته. ولا يعد من هذا القبيل قيام الجاني بالتحرش بالمجني عليه، فتلك جريمة أخرى هي جريمة التحرش وهي من الجرائم الأخلاقية. وليس للجاني الاحتجاج يكون المجني عليه لم يعلمه صراحة برغبته في عدم التواصل معه، لكون هذه الجريمة من الجرائم التي تمثل عدوانا على الحس الأخلاقي الإنساني الذي يجب أن يكون لدى كل إنسان.



الفصل السادس
الجوانب الإجرائية والتشريعية للجريمة المعلوماتية
ودور التعاون الدولى

يلزم للمجتمع المعلوماتى فى مجال قانون الاجراءات الجنائية أن ينشئ قواعد قانونية حديثة بحيث تضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق فى مجال جرائم الكمبيوتر.

والسبب فى ذلك أن محترفى انتهاك شبكات الحاسبات الآلية ومرتكبى الجرائم الاقتصادية وتجار الأسلحة والمواد المخدرة يقومون بتخزين معلوماتهم فى أنظمة تقنية المعلومات وعلى نحو متطور. وتصطدم الأجهزة المكلفة بالتحقيق بهذا التكنيك لتخزين المعلومات وهى التى تسعى للحصول على أدلة الاثبات.

وتصادف الصعوبات عندما يتعلق الأمر على وجه الخصوص بتخزين بيانات بالخارج بواسطة شبكة الاتصالات البعدية[1] .Telecommunication ويصعب حتى هذه اللحظة فى غالبية الأنظمة القانونية أن نحدد إلى أى مدى تكفى الأساليب التقليدية للإكراه فى قانون الإجراءات الجنائية من أجل مباشرة تحقيقات ناجحة فى مجال تقنية المعلومات . وقد اقترن بظهور تقنية المعلومات مشاكل خاصة ومستحدثة وعلى سبيل المثال التفتيش التحفظ على المعلومات

(1) وعلاوة على ذلك فإن غالبية الاجراءات الجنائية لا تكون كافية ولا مناسبة لأغراض التحقيق والحكم في هذا النمط من أنماط الجرائم. ومؤدى ذلك فيبدو من الضروري أيجاد اجراءات لديها القدرة على الملائمة مع المتطلبات الحديثة التي تفرضها تكنولوجيا المعلومات راجع في ذلك : La criminamite informatique sur l'internet

والزام الشاهد باسترجاع وكتابة المعلومات والحق فى مراقبة وتسجيل البيانات المنقولة بواسطة أنظمة الاتصالات البعدية وجمعها وتخزينها وضم المعلومات الإسمية إلى الدعوى الجنائية.

ونظرا لسهولة حركة المعلومات فى مجال أنظمة تقنية المعلومات حيث تجعل هذه السهولة لحركة المعلومات أنه بالإمكان ارتكاب جريمة عن طريق حاسب ألي موجود فى دولة معينة بينما يتحقق نتيجة هذا الفعل الاجرامى فى دولة أخرى.

لذا يقتضى الأمر ضرورة وجود تعاون دولى محكم فى مجال مكافحة هذا النوع من الجرائم ولأجل توفير حماية حقيقية لأنظمة الاتصالات البعدية.

على أية حال ينقسم هذا الفصل إلى ثلاثة مباحث، اختص المبحث الأول منها بمعالجة إجراءات جمع الأدلة بخصوص جريمة سرقة المعلومات فيما تناول الثانى معوقات جمع الأدلة فى مجال جريمة سرقة المعلومات أما الثالث فقد عكف على بيان دور التعاون الدولي في مجال مكافحة الجريمة المعلوماتية.



المبحث الأول

إجراءات جمع الأدلة بخصوص جريمة سرقة المعلومات

إجراءات التحقيق هى مجموعة الأعمال التى يرى المحقق وجوب أو ملائمة القيام بها لكشف الحقيقة بالنسبة لواقعة معينة يهتم بها قانون العقوبات .

وتنقسم هذه الإجراءات إلى قسمين: قسم يهدف إلى الحصول على الدليل كالتفتيش وسماع الشهود وقسم يمهد للدليل ويؤدى إليه كالقبض والحبس الاحتياطى.

وتسمى المجوعة الأولى : إجراءات جمع الأدلة أما الثانية: فتعرف بالإجراءات الاحتياطية ضد المتهم.

وسوف يقتصر دراستنا على الإجراءات الخاصة بجمع الأدلة وهذه إجراءات تنطوي أيضا على المساس بالحريات وهذا أبرز ما يميز ولهذا فإنه يجب النظر اليها باعتبارها واردة على سبيل الحصر فلا يجوز للمحقق أن يباشر إجراء آخر فيه مساس بحريات الأفراد ولو كان من شأنه أن يؤدى إلى كشف الحقيقة كإستعمال جهاز كشف الكذب أو مصل الحقيقة.

وإجراءات جمع الأدلة كما حددها القانون هى : المعاينة, ندب الخبراء , التفتيش, وضبط الأشياء ومراقبة المحادثات وتسجيلها وسماع الشهود والاستجواب والمواجهة.

وليس على المحقق التزام باتباع ترتيب معين عند مباشرة هذه الإجراءات بل هو غير ملزم أساسا لمباشرتها جميعا وأنما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتبها وفقا لما تقضى به هذه المصلحة وما تسمح به هذه الظروف.

- معاينة مسرح الجريمة والمعلوماتية:

يقصد بالمعاينة فحص مكان أو شئ أو شخص له علاقة بالجريمة وإثبات حالته[1]. كمعاينة مكان ارتكاب الجريمة أو أداة ارتكابها أو محلها أو معاينة جسم أو ملابس الجانى أو المجنى عليه لإثبات ما بالجسم من جراح وما على الثياب من دماء أو ما بها من مزق أو ثقوب.

ويلاحظ أن المعاينة قد تكون إجراء تحقيق أو استدلال , ولا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد , فإذا جرت المعاينة فى مكن عام كانت إجراء استدلال , وإذا اقتضت دخول مسكن أو له حرمة خاصة كانت إجراء تحقيق[2].

---

(1) توجب المادة 35 من قانون الإجراءات الجزائية الإماراتي، على مأموري الضبط القضائي وعلى مرؤوسيهم ، أجراء المعاينة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعملون بها بأية كيفية كانت.

وتقضي المادة 43 من القانون ذاته وأنه على مأموري الضبط القضائي في حالة التلبس بجريمة أن ينتقل فورا لمحل الواقعة ويعاين الأثار المادية للجريمة ويحافظ عليها ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيق .. وعليه إخطار النيابة العامة فورا بانتقاله ، وعلى النيابة العامة الانتقال فورا إلى محل الواقعة بمجرد إخطارها بجناية متلبس بها.

كما تنص المادة 90 من قانون الإجراءات الجنائية المصري على أن ينتقل قاضي التحقيق إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة ماديا وكل ما يلزم إثبات حالته والمقصود بهذاالنص تيسير مهمة المحقق وتمكينه من انجاز التحقيق بالسرعة اللازمة قبل أن تندثر معالم الجريمة أم تطمس أدلتها فيتعذر الوصول إلى الحقيقة بعد ذلك .

(2) انظر في ذلك :

د. عوض محمد – قانون الإجراءات الجنائية – الجزء الأول 1989 مؤسسة الثقافة الجامعية ص470 وما بعدها.

والمعاينة جوازية للمحقق شأنها شأن سائر إجراءات التحقيق فهى متروكة الى تقديرة سواء طلبها الخصوم أو لم يطلبوها.

ولا تتمتع المعاينة فى مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التى تلعبها فى مجال الجريمة التقليدية[1]. ومرد ذلك فى اعتبارين:

الأول : أن الجرائم التى تقع على نظم المعلومات والشبكات قلما أن يترتب على ارتكابها آثار مادية.

الثانى : أن عددا كبيرا من الأشخاص قد يتردد على مكان أو مسرح الجريمة خلال الفترة الزمنية التى تتوسط عادة ارتكابها الجريمة واكتشافها مما يهئ الفرصة لحدوث تغيير أو أتلاف أو عبث بالآثار المادية[2].

---

(1) انظر في ذلك

د. محمد محمد عنب، معاينة مسرح الجريمة – رسالة دكتوراه أكاديمية الشرطة – كلية الدراسات العليا القاهرة – 1988 ، ص13 ، وما بعدها

(2) تنص المادة 266 عقوبات اتحادي فتقضي بأن يعاقب بالحبس كل من غير بقصد تضليل القضاة حالة الأشخاص أو الأماكن أو الأشياء أو أخفى أدلة الجريمة أو قدم معلومات كاذبة تتعلق بها وهو يعلم عدم صحتها كما تنص المادة 286 من القانون اته على أن من أخفى أو أوى بنفسه أو بواسطة غيره شخصا في بعج القبض عليه أو متهما في جريمة أو صادرا في حقه أمر بالقبض عليه ، وكذلك كل من أعانه بأية طريقة كانت على الفرار من وجه العدالة مع علمه بذلك يعاقب طبقا للأحوال الآتية .. " وتقضي المادة 287 من ذات القانون أيضا بأن من علم بوقوع جريمة وأعان مرتكبيها على الفرار من وجه العدالة بإخفاء دليل من أدلة الجريمة... أو أعانه بأية طريقة أخرى يعاقب طبقا للأحوال الأتية .. " كما تنص المادة 145 عقوبات مصري على أنه كل من علم بوقوع جناية أو جنحة أو كان لديه ما يحمل معلى الاعتقاد بوقوعها وأعان الجاني بأية طريقة كانت على الفرار من وجه القضاء إما بإيواء الجاني المذكور وإما بإخفاء أدلة الجريمة أو بتقديم معلومات تتعلق بالجريمة وهو يعلم بعدم صحتها أوة كان لديه ما يحمله على الاعتقاد بذلك يعاقب .. ".

أو زوال بعضها وهو ما يثير الشك فى الدليل المستمد من المعاينة وحتى تصبح معاينة مسرح الجريمة المعلوماتية لها فائدة فى كشف الحقيقة عنها وعن مرتكبها فإنه ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلى:

1- تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته ويراعى تسجيل وقت وتاريخ ومكان التقاط كل صورة.

2- العناية البالغة بملاحظة الطريقة التى تم بها إعداد النظام والآثار الالكترونية وبوجه خاص السجلات الالكترونية التى تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذى تم عن طريقه الولوج إلى النظام أو الموقع أو الدخول معه فى حوار.

3- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن أجراء عملية المقارنة والتحليل حن عرض الأمر فيما بعد على القضاء.

4- عدم نقل أية مادة معلوماتية من مسرح الجريمة قبل أجراء إختبارات للتأكد من خلو المحيط الخارجى لموقع الحاسب من أى مجالات لقوى مغناطيسية يمكن أن تتسبب فى محو البيانات المسجلة.

5- التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة أو المحطمة وفحصها ورفع البصمات التى قد تكون لها صله بالجريمة المرتكبة.

6- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليه من بصمات[1].

(1) راجع في ذلك :

د. هشام محمد فريد رستم سابق الإشارة إليه ، ص104 وما بعدها.

7- اعداد خطة الهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق على أن تكون الخطة موضحة بالرسومات ةتتم مراجعتها مع أعضاء الفريق قبل بدء التحرك مع الأخذ فى الاعتبار قاعدة smeac العسكرية والتى تعنى الحالة (situation) الرسالة (mission) التنفيذ (execution) المداخل والمخارج (avenues of approach) والاتصالات (communication) وهى ملائمة ل؟لأجهزة الأمنية أحهزة تنفيذ القوانين فالحالة أو الوضع يعنى معرفة حجم القضية التى تقوم بالتحقيق فيها, وعدد المتورطين فيه أما الرسالة فهى تحديد الهدف من الغاره والتنفيذ يعنى كيفية أداء المهمة أما المداخل والمخارج فإن معرفتها ضرورية وهى تختلف من جريمة لاخرى وتحسب وفقا لمكونات طريق التحقيق بينما يأتى عنصر الاتصالات لضمان السرية وسلامة التعامل وتبادل المعلومات أثناء عملية الغارة.

وبعد وصول الفريق إلى مسرح الجريمة أو مكان الغارة يتم التأمين والسيطرة على المكان والبدء فى التفتيش على النحوالتالى :

أ- السيطرة على المناطق المحيطة بمسرح الجريمة أو مكان الإغارة وذلك طريق إغلاق الطرق والمداخل.

ب- السيطرة على الدائرة المحيطة بمكان الإغارة بوضع حراسات كافية لمراقبة التحركات داخل الدائرة ورصد الاتصالات الهاتفية من وإلى مكان الإغارة مع أبطال أجهزة الهاتف النقال.

ج- تأمين موقع الغارة والسيطرة على جميع أركانها ومنافذها والتحفظ على الأشخاص الموجودين.

د- تحديد أجهزة الحاسب الآلى الموجودة فى مكان الأغارة وتحديد مواقعها بأسرع فرصة ممكنه وفى حالة وجود شبكة إتصالات يجب البحث عن خادم الملف file server لتعطيل حركة الاتصالات.

و- يوضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من إتلاف المعلومات من على البعد أو من جهاز آخر داخل المبنى

هـ- إختيار مكان لمقابلة المتهمين والشهود على أن يكون المكان بعيدا عن أجهزة الحاسب الآلى[1].

- التفتيش فى مجال الجريمة المعلوماتية:

التفتيش فى قانون الاجراءات هو البحث عن شئ يتصل بجريمة وقعت ويفيد فى كشف الحقيقة عنها وعن مرتكبيها, وقد يقتضى التفتيش إجراء البحث فى محل له حرمة خاصة, وقد أحاط القانون هذا التفتيش بضمانات عديدة. ومحل التفتيش إما أن يكون مسكنا أو شخصا, وهو بنوعيه قد يكون متعلقا بالمتهم أو بغيره وهو فى كل أحواله جائز مع إختلاف فى بعض الشروط[2].

- مدى قابلية مكونات وشبكات الحاسب الآلى للتفتيش:

يتكون الحاسب الآلى من مكونات مادية Hard Dware مكونات منطقية soft ware كما أن له شبكات اتصالات بعدية سلكية ولا سلكية سواء على المستوى المحلى أو المستوى الدولى فهل تخضع هذه المكونات للتفتيش؟

أولا: مدى خضوع مكونات الحاسب المادية للتفتيش

يخضع الولوج فى المكونات المادية للحاسب بحثا عن شئ يتصل بجريمة معلوماتية وقعت ويفيد فى كشف الحقيقة عنها وعن مرتكبها

---

(1) راجع في ذلك :

د. محمد الأمين البشري التحقيق في جرائم الحاسب الآلي بحث مقدم إلى مؤتمر القانون والانترنت بتاريخ 3 مايو 2000 لجامعة الإمارات ص30.

(2) انظر في ذلك :

د. عوض محمد سابق الإشارة إليه ص475.

للإجراءات القانونية الخاصه بالتفتيش . وبعبارة أخرى فإن جواز تفتيش تلك المكونات يتوقف على طبيعة المكان الموجوده فيه التفتيش وهل هو مكان عام أم مكان خاص إذ أن لصفة المكان أهمية خاصه فى مجال التفتيش فإذا كانت موجوده فى مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا فى الحالات التى يجوز فيها تفتيش مسكنه وبنفس الضمانات المقرر قانونا فى التشريعات المختلفة.

ويجب التميز داخل المكان الخاص بين ما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحاسبات الأخرى أم أنها متصله بحاسب أ بنهاية طرفية terminal فى مكان أخر كمسكن لا يخص مسكن المتهم. فإذا كانت هناك بيانات مخزنة فى أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التى يستلزمها المشرع لتفتيش هذه الأماكن . أما بالنسبة للأماكن العامة, فإذا وجد شخص وهو يحمل مكونات الحاسب الآلى المادية أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا فى الحالات التى يجوز فيها تفتيش الأشخاص بنفس الضمانات والقيود المنصوص عليها فى هذا المجال.

ومن التشريعات التى تجيز تفتيش مكونات الحاسب الآلى نذكر المادة 251من قانون الاجراءات الجنائية اليونانى[1]. والمادة487 من قانون الاجراءات.

الكندى[2]. وهناك قله من التشريعات تنص صراحة على تفتيش مكونات الحاسب الآلى من ذلك القانون الانجليزى السابق سنة 1990 والذى يطلق

---

(1) Vassilaki (Irini): computer crimes and other crimes against information technology in Greece RI.D.P. 1993,P.371

مشار إليه د. هلالي عبد اللـه أحمد، تفتيش الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربيـة، القاهرة 1997، ص74.

(2) pirgoff (Donoldk): computer crimes and other crimes against information technology in Canada R.I.D.P. 1993,P.241

عليه قانون إساءة استخدام الحاسب computer misuse[1] كذلك هناك بعض القوانينالتى تحتوى على قواعد تفصيلية للتفتيش تطبق على مكونات الحاسب وبياناته فى حالات معينة ومن ذلك على سبيل المثال القسم رقم 16 -1 من قانون المنافسة competition فى كندا حيث يمنح الشخص T. C. A. الذى يحمل إذن بالتفتيش الحق فى أن يستخدم أى نظام للحاسب الآلى لتفتيش أى بيانات يحتويها أو تكون متاحه لهذا النظام أو يجوز له أن يسجل أو يعمل على تسجيل تلك البيانات فى شكل مطبوعات أى مخرجات أخرى[2].

ثانيا: مدى خضوع مكونات الحاسب المعنوية للتفتيش

بالنسبة لتفتيش مكونات الحاسب المعنوية فقد ثار الخلاف بشأن جواز تفتيشها حيث يذهب رأى أنه اذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التى تفيد فى كشف الحقيقة فإن هذا المفهوم يمتد ليشمل البيانات الالكترونية بمختلف أشكالها. وفى هذا المعنى نجد المادة 251 من قانون الاجراءات الجنائى اليونانى تعطى سلطات التحقيق أمكانية القيام (بأى شئ يكون ضروريا لجمع وحماية الدليل) ويفسر الفقه اليونانى عبارة أى شئ بأنها تشمل ضبط البيانات المخزنة أو المعالجة اليكترونيا. ولذلك فإن ضبط البيانات المخزنة فى الذاكرة الداخلية للحاسب الآلى لا تشكل أية مشكلة فى اليونان إذ بمقدور المحقق أن يعطى أمرا للخبير بجمع البيانات التى يمكن أن تكون مقبوله كدليل فى المحاكمة الجنائية[3].

---

(1) ferbrache (david): Pathology of computer viruses springer verly London L.T.D. 1992,P.233

(2) DURAM (COLO) : The emerging strucrues of criminal information law tracing the contours of a new poraigm R.I.D.P.1993,P.111

(3) راجع في ذلك :
د. هلالي عبد اللاه أحمد سابق الإشارة إليه ص 82.

وتمنح المادة 487 من القانون الجنائى الكندى سلطة اصدار إذن لضبط أى شئ طالما تتوافر أسس معقولة للإعتقاد بأن الجريمة إرتكبت أو يشتبه فى ارتكابها أو أن هناك نية فى أن يستخدم فى ارتكاب الجريمة أو أنه سوف ينتج دليلا على وقوع الجريمة.

وهكذا يفسر هذا النص بوضوح على أنه يسمح بضبط بيانات الحاسب غير المحسوسه[1].

وهناك على النقيض رأى أخر يرى أنه إذا كانت الغاية من التفتيش هى ضبط الأدلة المادية التى تفيد فى كشف الحقيقة فإن هذا المفهوم المادى لا ينطبق على بيانات الحاسب الآلى غير المحسوسة أو الملموسة .

ويقترح هذا الرأى فى مواجهة هذا القصور التشريعى ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (المواد المعالجة عن طريق الحاسب الآلى أو بيانات الحاسب الآلى) وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقنى الحديث هى(البحث عن الأدلة المادية أو أى مادة معالجة بواسطة الحاسب)[2].

ويرى بعض الفقهاء فى فرنسا أن النبضات الالكترونية Electronic Im-pulse أو الاشارات الالكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة وبالتالى لا تعتبر شيئا ماديا بالمعنى المألوف للمصطلح[3]. ولذا لا يمكن ضبطة.

---

(1) راجع في ذلك :

د. هلالي عبد اللاه أحمد سابق الإشارة إليه ص 83

(2) انظر في ذلك :

د. هلالي عبد اللاه أحمد سابق الإشارة إليه ص 84

(3) انظر في ذلك :

Linformatique . J.c.P. 1989 3333 no. 16

Gassin (R) le droit penal et linformatiqe D.1982.p.38

وفى الولايات المتحدة الامريكية تم تعديل القاعدة رقم 34 من القواعد الفيدراليه الخاصه بالاجراءات الجنائية عام 1970 لتنص على السماح بتفتيش أجهزة الكمبيوتر والكشف عن الوسائط الالكترونية بما فة ذلك البريد الالكترونى والبريد الصوتى والبريد المنقول وعن طريق الفاكس[1].

ويتركز أذون التفتيش القياسية الصادرة عند التفتيش فى أحدى جرائم الكمبيوتر - وبصفة خاصة - على ضبط الوثائق المكتوبة إضافة إلى أجهزة الكمبيوتر وتتضمن هذه الوثائق على وجه التحديد: النسخ الضوئية, مطبوعات الكمبيوتر , فواتير التليفون, سجلات العناوين , المذكرات والمراسلات[2].

ثالثا: مدى خضوع شبكات الحاسب للتفتيش:

ويمكن فى الفرض التمييز بين ثلاث احتمالات :

- **احتمال الأول:** اتصال حاسب المتهم بحاسب أو نهاية طرفية موجوده فى مكان أخر داخل الدولة : ويرى الفقه الالمانى بشأن مدى أمكانية امتداد الحق فى التفتيش اذا تبين أن الحاسب أو النهاية الطرفية فى منزل المتهم متصلة بجهاز أو طرفية فى مكان أخر مملوك لشخص غير المتهم أنه يمكن أن يمتد التفتيش فى هذه الحالة إلى سجلات البيانات التى تكون فى موقع أخر استنادا إلى مقتضيات القسم 103 من قانون الاجراءات الجنائية الالمانى[3].

(1) راجع في ذلك :

Linda volonino ibid, p.2

(2) انظر في ذلك :

Brucisterling , ibid, p. 165

(3) KASPERSEN (W.K. Henrik): computer crimes and other crimes against information technology in the Netherlands R.I.D.P.1993,P.479

كما نص مشروع قانون جرائم الحاسب الآلى فى هولندا[1]. على جواز أن يمتد التفتيش إلى نظم المعلومات الموجودة فى موقع أخر بشرط أن تكون البيانات الخاصه به ضرورية لإظهار الحقيقة (القسم الخامس من المادة125) وذلك بمراعاة بعض القيود.

- **الاحتمال الثانى:** اتصال حاسب المتهم بحاسب أو نهاية طرفية موجوده فى مكان أخر خارج الدولة : من المتصور طبقا لهذا الاحتمال أن يقوم مرتكبى الجرائم بتخزين بياناتهم فى أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الاتصالات البعديه بهدف عرقلة سلطات الادعاء فى جمع الأدلة.ولمواجهة هذا الاحتمال نص مشروع قانون جريمة الحاسب الآلى بهولندا أنه يجوز لجهات التحقيق مباشرة التفتيش داخل الأماكن وبما ينطوى عليه تفتيش نظم الحاسب المرتبطه حتى إذا كانت موجودة فى دول أخرى وبشرط أن يكون هذا التدخل مؤقتا وأن تكون البيانات التى يتم التفتيش عنها لازمة لإظهار الحقيقه (المادة 125)[2].

ووفقا لما جاء بتقرير المجلس الأوربى فإن هذا الاختراق المباشر يعتبر إنتهاكا لسيادة دولة أخرى مالم توجد إتفاقية دولية فى هذا الشأن ويؤيد الفقه الالمانى ما جاء بتقرير المجلس الأوربى حيث أن السماح بإسترجاع البيانات التى تم تخزينها بالخارج يعتبر انتهاكا لحقوق السيادة لدولة أخرى وخرقا للقوانين الثنائية والوطنية الخاصة بامكانية التعاون فى مجال العدالة القضائيه[3]. وقد أيد القضاء الالمانى هذا الاتجاه حيث أسفر البحث فى احدى

(1) راجع في ذلك :

د. هلالي عبد اللاه أحمد سابق الإشارة إليه ص 77

(2) DURHAM (COLO) : the emerging structures of criminal infromatin law : tracing the contours of a new paradigm general report for the a.i.d.p. collwuium R.I.D.P. 1993.P.115

(3) راجع في ذلك

جرائم الغش المعلوماتى عن وجود طرفية حاسب فى المانيا متصله بشبكة اتصالات فى سويسرا حيث يتم تخزين بيانات المشروعات فيها وعندما أرادت سلطات التحقيق الالمانية الحصول على هذه البيانات لم يتحقق لها ذلك الا من خلال طلب المساعدة المتبادلة request for mutual assistance[1]. وقد ساور الاعتقاد الشرطة اليابانية بأن مجموعة من المخربين قد استخدمت أجهزة الكمبيوتر فى الصين والولايات المتحدة فى مهاجمة العديد من المواقع الخاصة للحكومة اليابانية على الشبكة وقد طالبت الشرطة اليابانية كل من بكين وواشنطن بتسليم بيانات الدخول المسجلة على أجهزة الكمبيوتر فى كل من هاتين الدولتين حتى يتمكنوا من الوصول إلى جذور هذه العملية الارهابية[2].

- **احتمال الثالث:** يسمح بالتصنت WIREAPPING والاشكال الأخرى للمراقبة التليفونية فى العديد من الدول[3]. حيث يجيز القانون الفرنسى الصادر فى 10 يوليو سنة 1991 لعتراض الاتصالات البعدية(telem atiqe) بما فى ذلك شبكات تبادل المعلومات[4]. ويجوز لقاضى التحقيق فى هولندا أن يأمر بالتصنت على شبكات اتصالات الحاسب اذا كانت هناك جرائم خطيرة متورط فيها المتهم وتشمل هذه الشبكة التلكس

=

Mohrenschl ager (Mnfred) : computer crimes and other crimes against information technology in Germany r.i.d.p.1993,p.351

(1) ibid.p. 365.

(2) راجع في ذلك :

Linda volonio ibid., p.4.

(3) راجع في ذلك :

DURHAM (COLO) op.cit., p. 113

(4) راجع في ذلك :

Dr: Jacques francillon . op.cit. 304

والفاكس ونقل البيانات Data communication [1].وفى الولايات المتحدة الأمريكية - يجوز اعتراض الاتصالات الالكترونية بما فيها شبكات الحاسب بشرط الحصول على إذن تفتيش صادر من القاضى[2].

- ضوابط تفتيش نظم الحاسب الآلى

يمكن تقسيم ضوابط تفتيش نظم الحاسب الآلى إلى نوعين : الأولى موضوعية والأخرى: شكلية.

أولا : الضوابط الموضوعية لتفتيش نظم الحاسب الآلى

وتنحصر هذه الضوابط فى :

أ- وقوع جريمة ملوماتية: والجريمة المعلوماتية هى كما سبق القول كل فعل غير مشروع مرتبط باستخدام الحاسب الآلى لتحقيق أغراض غير مشروعة[3].

وهناك العديد من التشريعات التى حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لإنجلترا والتى أصدرت قانون اساءة استخدام الحاسب الآلى computer misuse act فى 29 يونيو 1990[4].وفى الولايات المتحدة الأمريكية حيث صدر قانون الاحتيال واساءة

---

(1) KASPERSEN (W.K.Henrik) : Computer crimes and other crimes against information technology in the nether lands r.i.d. p. 1993,p.500

(2) راجع في ذلك :

BRUCITERLING ibid, p. 165

(3) انظر في ذلك : د. محمد سامي الشواء، سابقا الإشارة إليه ، ص8

د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ، ص30

(4) this act made it acriminal offence for anyone to acces of to modify computer held data or software without authority , or attempt to do so .
It created three specific offenceses .

استخدام الحاسب الآلى سنة 1986 والذى طبق على المستوى الفيدرالى[1]. بالاضافة الى قوانين بعض الولايات الامريكية كقانون ولاية تكساس الصادر فى أول سبتمبر سنة 1985 بشأن الدخول غير المشروع فى نظام الحاسب وفى فرنسا صدر قانون رقم 19-88 فى 5 يناير سنة 1988 وهو الخاص بالغش المعلوماتى[2]. والذى تم تعديله مع صدور قانون العقوبات الفرنسى الجديد الذى بدأ العمل به اعتبارا من أول مارس سنة 1994 وفى الدنمارك صدر قانون جرائم الحاسب فى 6 يونيو سنة 1985.

وقد أدرج المشرع الاماراتى برامج الحاسب ضمن المصنفات الفكرية المحمية بالقانون الاتحادى رقم 40 لسنة 1992 كذلك اعتبر المشرع المصرى مصنفات الحاسب الآلى من برامج وقواعد بيانات وما يماثلها من

=

1- Accessis delibnerate and unothorieses.

2- Access is without authority and with attention to commit afurther offense (either immediately or in the future).

3- A person does and eliberte act that causes and unaut horises modification of the computers content

وهناك عدة ملاحظات على نصوص هذا القانون وهي :

- إن التآمر والشروع والتحريض تعد جميعها من بين الجرائم .
- لا يلزم الادعاء بالحصول على دليل يفيد بأن تلك الأفعال قد تم توجيهها صوب بنود معينة من البيانات أو البرامج.
- لا يلزم وجود المتهم في المملكة المتحدة وقت ارتكاب الجريمة.
- لا يلزم وجود بيانات الكمبيوتر المستهدفة في المملكة المتحدة.

(1) راجع في ذلك :

Jackson (K.M.), HRUSKA (Op.cit.,passim.,pp.) : Computer security refernce book editor donn B. Parker 1992,p.401

(2) راجع في ذلك :

Chamaux (Francais) la loi sur la fraude infromatique de nouvelles incriminations J.C.P. 1988-1-3321.

مصنفات تحدد بقرار من وزير الثقافة ضمن المصنفات المشمولة بحماية حق المؤلف المنصوص عليها فى المادة الثانية بمقتضى القانون رقم 38 لسنة 1992.

ب- تورط شخص أو أشخاص معينين فى ارتكاب الجريمة المعلوماتية أو الاشتراك فيه: ينبغى أن تتوافر فى حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم فى ارتكاب الجريمة المعلوماتية سواء بوصفه فاعلا لها أو شريكا فيها وفى مجال الحاسب الآلى يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر أو الامارات المعنية التى تقوم على المضمون العقلى والمنطقى لملابسات الواقعة وكذلك على خبرة وحرفية القائم بالتفتيش والتى تؤيد نسبة الجريمة المعلوماتية إلى شخص سواء بوصفه فاعلا أو شريكا.

ج- توافر أمارات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد فى كشف الحقيقة لدى المتهم . لا يوجد التفتيش إلا إذا توافرت لدى المحقق أسباب كافية على أنه يوجد فى مكان أو لدى الشخص المراد تفتيشه أدوات استخدمت فى الجريمة المعلوماتية أو أشياء متحصلة منها. أو مستجدات الكترونية يحتمل أن يكون لها فائدة فى استجلاء الحقيقة لدى المتهم أو غيره إذ من المقرر أن كل ما يشترط لصحة التفتيش الذى تجربه النيابة أو تأذن فى اجرائه فى مسكن المتهم أو ما يتصل بشخصه هو أن يكون رجل الضبط القضائى قد علم من تحرياته واستدلالاته أن جريمة معينة - جناية أو جنحة - قد وقعت من شخص معين أو أن تكون هناك من الدلائل والامارات الكافية والشبهات المقبولة ضد هذا الشخص بقدر يبرر تعرض التفتيش لحريته أو لحرمة مسكنه فى سبيل كشف اتصاله بالجريمة المعلوماتية[1].

(1) نقض 26 يناير سنة 1981 مجموعة احكام النقض س 50 رقم 12 ص79.

د- ومحل التفتيش الخاص بنظم الحاسب الآلى هى كل مكونات الحاسب سواء كانت مادية أو معنوية أو شبكات الاتصال الخاصة به بالاضافة إلى الأشخاص الذين يستخدمون الحاسب الآلى محل التفتيش.

وتشمل المكونات المادية للحاسب وحدة الإدخال Input ووحدة الذاكرة الرئيسية Main Memory ووحدة الحساب والمنطق Arithmatic and logic unit وحدات الاخراج Output وأخيرا وحدات التخزين الثانوية Secondary age Units.

كما تنقسم المكونات المعنوية للحاسب إلى الكيانات المطقية الأساسية أو برامج النظام والكيانات المنطقية التطبيقية أو برامج التطبيقات بنوعيها برامج التطبيقات سابقة التجهيز وبرامج التطبيقات طبقا لاحتياجات العميل, ويستلزم الحاسب بمكوناته سالفة الذكر مجموعة من الأشخاص لديهم خبرة ومهارة فى تقنية نظم المعلومات وهم مشغلو الحاسب computer aperators وخبراء البرامج programmers سواء كانوا مخططى برامج تطبيقات أم كانوا مخططى برامج نظم والمحللين ومهندسى الصيانة والاتصالات ومديرى النظم المعلوماتية.

ثانيا: الضوابط الشكلية لتفتيش نظم الحاسب الآلى:

أ- **الأسلوب الآلى لتنفيذ التفتيش فى نظم الحاسب الآلى :** نظم القانون الأمريكى أسلوب تنفيذ التفتيش فى نظم الحاسب الآلى وذلك على النحو التالى:

تقتحم قوات الشرطة المكان بصورة سريعة ومن كافة منافذة فى أن واحد وذلك بإستخدام القدر الأعظم من القوة بإفتراض أن هذا التكتيك يقلل من احتمالية وقوع اصابات بين صفوف رجال الشرطة .

يتم إبعاد سائر المشتبه فيهم عن كافة أنظمة ومعدات الكمبيوتر المتواجد فى المكان على الفور حتى لا يتمكنوا من تشويه أو تدمير أى دليل الكترونى, ويتم ادخال سائر المشتبه فيهم إلى غرفة لا توجب بها أية أجهزة كمبيوتر, ودائما ما تكون غرفة المعيشة ويوضعوا تحت حراسة مشددة, وفى هذه الخطوة يتم تقديم إذن التفتيش الصادر من النيابة اليهم ويتم تحذيرهم بأن كافة أقوالهم

ستحسب عليهم منذ هذه اللحظة وقد تؤخذ بمثابة دليل ادانة ضدهم ودائما ما سنجد لدى العديد منه الكثيرمن الحديث وخاصة إذا ما كانوا أولياء أمور غافلين عن حقيقة ما يحدث بمنزلهم . وفى مكان ما من المنزل , سنجد النقطة الساخنة - جهاز كمبيوتر متصل بخط تليفونى أو ربما نجد أكثر من جهاز وأكثر من خط فى المنزل الواحد , وعادة ما تكون هذه النقطة الساخنة داخل غرفة النوم الخاصة بأحد الأبناء المراهقين (أو بأى مكان آخر داخل المنزل).

توضيح النقطة الساخنة في عهدة فريق يضم اثنين من العملاء ،"مكتشف "و"مسجل " ويجب أن يكون المكتشف من بين العملاء الذين تم تدريبهم تدريبا متقدما على نظم المعلومات ودائما ما يقوم بهذا الدور العميل المعنى القضية بالقضية والذي عاصرها من البداية واستصدر إذن التفتيش الخاص بها من القاضي فهذا الشخص يعرف تماما الشئ أو الأشياء التي يبحث عنها ويتفهم طبيعتها تماما ولن نتجاوز إذا ما قلنا أنه هو الذي يقوم بعملية الضبط .ويتولى المكتشف نزع مقيس الكهرباء الخاص بسائر الأجهزة ويقوم بفتح الأدراج والبحث عن الديسكات والملفات وحاويات الاسطوانات...إلخ.

أما المسجل فيتولى تصوير كافة الأجهزة والمعدات على ذات الكيفية التي تم ضبطها عليها- وبخاصة وصلات الأسلاك المتشابكة الملقاة خلف الأجهزة (حتى يتمكن الفريق من اعادة تجميعها على ما كانت عليه).

ويقوم المسجل كذلك عادة بتصوير كافة الغرف الأخرى الموجودة بالمنزل حتى لا يدعى أحد المجرمين الماكرين أن الشرطة قد سرقت منزله أثناء التفتيش، ويحمل بعض المسجلين كاميرات فيديو أو أجهزة تسجيل صوتي ويتم توصيف الأشياء .والتي تم العثور عليها وترقيمها ودائما ما يتم ذلك على استمارة مطبوعة معممة الاستخدام في سائر أجهزة الشرطة[1].

---

(1) انظر في ذلك :

Brucistercing ibid,p.165

ب- فريق التفتيش: وهو الفريق المعنى باجراءات التحقيق وهو جزء داخل فريق الاغارة الذي يضم بجانب فريق التفتيش والضبط رجال الحراسات والأمن وقوات الحماية والتأمين ورجال المباحث والمراقبة السرية والمعاونين من العمال والعمال المهرة والسائقين وخبراء مسرح الجريمة العادية الملائمين للجريمة موضوع التحقيق .ويتكون فريق التفتيش والضبط من :

- المشرف على التحقيق :

والجزء يجب أن يكون من ذوي الخبرات الطويلة في مجال التحقيق الجنائي في الجرائم المعقدة ويتولى المشرف إدارة العمل في مسرح الجريمة وتوزيع المهام على أعضاء الفريق .

- فريق أخذ الافادات :

ويحدد عدد أعضاء هذا الفريق حسب حجم الجريمة والمتورطين فيها وعدد الشهود الذين قد يتواجدون في مسرح الجريمة وعليه قد يكون الفريق من شخصين أو أكثر .

- فريق الرسم والتصوير :

ويضم شخصا أو أكثر يقومون برسم الخرائط الكروكية لمسرح الجريمة وتحديد مواقع الأجهزة والملفات والاشخاص والتقاط الصور الفوتوغرافية والتصوير بالفيديو-مع مراعاة أن يتم تنبيه جميع العاملين في مسرح الجريمة عند استعمال الفيديو تحسبا لتسجيل أصوات المشاركين في التفتيش.

- فريق التفتيش العلمي :

ويضم شخصا واحدا أكثر حسب الاحوال ويتولى هذا الفريق عملية البحث والدقيق على مسرح الجريمة وفقا للنظم الفنية التي تتبع في تفتيش الأماكن وتفتيش مسرح الجريمة ويقوم هذا الفريق بالمرور على جميع

الغرف والمخازن ويفحص المخازن والمخابئ وليس من الضروري أن يكون أعضاء هذا الفريق من خبراء الحاسب الآلي ولكن يفضل أن يتم تنويرهم بالأشياء التي ينبغي البحث عنها .

- فريق التأمين والقبض :

ويعني هذا الفريق بالسيطرة أمنيا على مسرح الجريمة وضبط مخارجها ومنافذها وحركة الموجودين في المبنى والمباني المجاورة لمسرح الجريمة ،وتنفيذ عملية القبض على المشتبه فيهم واحتجازهم وفق ما يأمر به المشرف ويتكون هذا الفريق من رجال الأمن بالزي الرسمي .

- فريق ضبط وتحريز الأدلة :

ويضم هذا الفريق اثنين أو أكثر من خبراء الحاسب الآلي يتولون ضبط وادخال المعلومات المضبوطة في الحاسب الآلي وتصنيف الأدلة وتحريزها في الصناديق ووضع العلامات الموضحة عليها ويقوم هذا الفريق بنقل أجهزة الحاسب الآلي المضبوطة بعد اجراءات الرسم والتصوير ويجب أن يكون من بين أعضاء هذا الفريق شخصان على الأقل أحدهما محقق في مجال الحاسب الآلي ،والثاني خبير في الحاسب الآلي على التعامل مع الأدلة وطرق تقييمها .

-خبراء مسرح الجريمة العادية:

يتم اختيارهم حسب الحال وقد يحتاج المحقق في بعض جرائم الحاسب الآلي كامل أعضاء الفريق أو بعضهم مثل خبراء البصمات المهندسين، خبراء المتفجرات [1]....إلخ.

(1) راجع في ذلك : د. محمد الأمين البشري، سابق الإشارة إليه ، ص30 وما بعدها.

- الشهادة في مجال الجريمة المعلوماتية

تعريف الشهادة وأهميتها :

الشهادة هي الأقوال التي يدلى بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها واسنادها إلى متهم أوبراءته منها[1]. وللشهادة في مجال الاجراءات أهمية بالغة لأن الجريمة ليست تطرفا قانونيا ولكنها عمل غير مشروع يجتهد الجاني في التكتم عند ارتكابه ويحرص على اخفائه عن الناس .

ولهذا فإن العثور على شاهد يعتبر مكسبا كبيرا للعدالة ومن هنا جاءت قاعدة عدم رد الشهود.

-تعيين الشهود واستدعاءهم :

سماع الشهود كسائر اجراءات التحقيق من الأمور التقليدية للمحقق فله أن يسمع الشهود أو يستغن عنهم فإذا قرر سماعهم فهو الذي يحدد من يجب الاستماع إليه ومن يمكن الاستغناء عنه والأمر متروك إلى فطنة المحقق ومرتبط بظروف التحقيق والأصل أن يطلب الخصوم سماع من يرون من الشهود غير أن للمحقق أن يجيبهم بل له أن يسمع شهادة أي شاهد يتقدم من تلقاء نفسه. ومن المبادئ المستقرة أن الشاهد لا يرد ولو غلب على الظن أنه لن يتحرى الصدق في شهادته سواء كان ذلك راجعا لانحطاط في خلقه أو لوجود صلة مودة أو لعداوة بينه وبين المتهم تجعله يميل له أو ضده .

---

(1) تعرف محكمة النقض المصرية الشهادة بأنها تقرير الشخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحراسه. (نقض 25-1-1976 أحكام النقض س27 ص94 رقم 20 و2978/2/2 س29ص139 رقم 25 و1979/4/2 س30ص426 رقم 90).

- المقصود بالشاهد في الجريمة المعلوماتية :

يقصد بالشاهد في الجريمة المعلوماتية الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام الجامعة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي وذلك تمييزا له عن ،الشاهد التقليدي ويشمل الشاهد المعلوماتي بهذا المفهوم عدة طوائف من أهمها :

1- القائم على تشغيل الحاسب الآلي

وهو المسئول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في ادخال البيانات كما يجب ان تكون لديه معلومات عن قواعد كتابة البرامج[1].

2- المبرمجون :

وهم الاشخاص المتخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين:

- **الفئة الأولى:** هم مخططوا برامج التطبيقات.
- **الفئة الثانية:** هم مخططوا برامج النظم.

حيث يقوم مخططو برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات. أما مخططو برامج النظم فيقوموا باختيار وتعديل

---

(1) انظر في ذلك :
د. محمد فهمي طلبة ، الموسوعة الشاملة لمصطلحات الحاسب الآلي الالكتروني ، القاهرة ، مطابع المكتب المصري الحديث ، سنة 1991 ، ص23

وتصحيح برامج نظام الحاسب الداخلية أي أنه يقوم بالوظائف الخاصة بتجهيز الحاسب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والاخراج ووسائط التخزين بالاضافة إلى إدخال أي تعديلات أو اضافات لهذه البرامج[1].

3- المحللون :

وهو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين ،ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات ،كما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب .

4-مهندسو الصيانة والاتصالات :

وهم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكونات وشبكات الاتصال المتعلقة به .

5-مدير النظم :

وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية [2].

ويحصر قانون الدليل الخاص بولاية كاليفونيا شهود الجريمة المعلوماتية في :

- محلل النظم الذي صمم وحدد برنامج الكمبيوتر الذي أنتج الدليل
- المبرمج الذي قام بتحرير البرنامج واختباره
- المشغل الذي يقوم بتشغيل البرامج .

---

(1) انظر في ذلك

د. محمد فهمي طلبه، سابق الإشارة إليه ، ص37.

(2) انظر في ذلك :

د. محمد فهمي طلبه، سابق الإشارة إليه ، ص23.

- طاقم عمليات البيانات الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أو اسطوانة)
- أمناء مكتبة الأشرطة الذين يتحملون مسئولية توفير الأشرطة أو الاسطوانات التي تشتمل على البيانات المصدرية الصحيحة
- مهندس الصيانة الالكترونية الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة صحيحة .
- موظفوا المدخلات والمخرجات والمسئولين عن معالجة المدخلات والمخرجات يدويا قبل وبعد أداء العمل .
- مبرمجوا صيانة النظام والمسئولون عن سرية عمل ويصرح عمل الكمبيوتر المستخدم في تنفيذ برامجه .

المستخدم النهائي الذي يمد بالمعلومات المدخلة ويصرح بتنفيذ برامج الكمبيوتر ويستخدم نواتجها[1].

التزامات الشاهد المعلوماتي :

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله . والسؤال الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات والافصاح عن كلمات المرور والشفرات ؟

هناك اتجاهان في هذا الصدد :

- **الاتجاه الأول:** ويرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الافصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة ويميل إلى هذا الاتجاه الالماني حيث

(1) بحث مقدم من مركز البحوث بشرطة دبي ، عام 1998 للإمارات العربية المتحدة.

يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام باداء الشهادة لا يتضمن هذا الواجب[1].

- **الاتجاه الثاني:** ويرى أنصار هذا الاتجاه أن من بين الالتزامات التي يتحمل بها الشاهد القيام ملفات البيانات أو الافصاح عن كلمات المرور او الشفرات الخاصة بالبرامج المختلفة[2] حيث يرى اتجاه في الفقه الفرنسي أن القواعد العامة في مجال الاجراءات تحتفظ بسلطانها في مجال الاجراءات المعلوماتية ومن ثمم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم (المواد 62، 109،138 من قانون الاجراءات الجزائية الفرنسي ومن ثم يجب عليهم الافصاح عن كلمات المرور السرية التي يعلمونها ،ولكن ربط اعطاء المعلومات المطلوبة غير معاقب جنائيا إلا في مرحلة التحقيق والمحاكمة[3] وفي هولندا يتيح مشروع قانون الحاسب الآلي لسلطات التحري والتحقيق أصدار الأمر للقائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله، كالافصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة وإذا وجدت بيانات مشفرة أو مرمزة داخل ذاكرة الحاسب وكانت مصلحة التحقيق تستلزم الحصول عليها ، يتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات[4].

---

(1) انظر في ذلك

Mohrenschlager (Manfred): "computer crimes and other crimes against information technology in germany ", R.I.D.P.1993P.351

(2) انظر في ذلك :

ERMAN (sahir) " les crimes infromatiques et d'autres crimes dans le domaine de la tecnologie infromatieque en torque , R.I.D.P. 1993,P.624

(3) راجع في ذلك :

DR.: Jacques franccillon op.cit.,p.309

(4) انظر في ذلك :

Kasbersen op.cit., p. 496.

وفي اليونان يمكن الحصول من القائم على تشغيل نظام الحاسب على كلمة المرور السرية للولوج في النظام المعلوماتي كما يمكن الحصول منه على بعض الإيضاحات الخاصة بنظامه الأمني لكن ليس على الشاهد أي التزاماته بالنسبة لطباعة ملفات بيانات مخزنة في ذلكرة الحاسب وذلك لانه يجب أن يشهد على معلومات حازها بالفعل وليس الكشف عن معلومات جديدة (المادة 323 فقرة 1 اجراءات جنائية يوناني)[1].

الخبرة في مجال الجريمة المعلوماتية

هنا من المقرر أن يتم ندب خبير مع مراعاة مبررات ندبه واجراءات هذا الندب، حيث يرى المحقق في بعض الأحيان ضرورة الاستعانة بالخبير لإيضاح مسألة تستعصي ثقافة العامة عن فهمها كتحديد سبب الوفاة أو ساعتها أو رفع بصمة وجدت في مكان الجريمة أو فحص سيارة لبيان ما فيها من خلل وتكتسب الخبرة أهمية بالغة في مجال الجريمة المعلوماتي نظرا لأن الحاسبات وشبكات الاتصال بينها على أنواع ونماذج متعددة كذلك فإن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات عملية وفنية دقيقة ومتنوعة والتطورات في مجالها سريعة ومتلاحة لدرجة قد يصعب معها على المتخصص تتبعها واستيعابها ويمكن القول بصفة عامة بأنه لا يوجد حتى الآن خبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرامجها وشبكتها كذلك لا يوجد خبير قادر على التعامل مع كاة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها[2].

---

(1) انظر في ذلك :

Vassilaki (Irini): computer crimes and other crimes against information technology in Greece , R.I.D.P.1993,P.371

(2) راجع في ذلك :

PHILIP M. stanely computer crime invetigatoin and investigators computer & security North Holland 1986,pp.310-311

مشار إليه في : د. هشام محمد فريد رستم، مرجع سابق الإشارة إليه.

لذا ترك المشرع للمحقق الحرية الكاملة في هذا الشأن ليمكنه من كشف الحقيقة بالسرعة اللازمة وبالطريقة التي يراها مناسبة[1] وللمحقق في أي وقت - إلى أن ينتهي التحقيق - أن يندب من يأنس فيه الكفاية الفنية اللازمة للاستعانة بخبرته.

وندب الخبير من سلطات المحقق فليس في القانون ما يلزمه بالاستجابة للمتهم ولا لغيره من الخصوم إذا طلبوا ندب الخبير.

يحدد المحقق للخبير مهمته والميعاد الذي فيه تقريره وعليه أن يحلفه اليمين على أن يبدى رأيه بالذمة وهذا الاجراء .جوهري يترتب على اغفاله بطلان عمل الخبير[2]. والأصل أن يباشر الخبير عمله في حضور المحقق وتحت اشرافه والاستثناء أن يتم في غيابه .

وللخصوم حق الحضور أثناء عمل الخبير ويجوز مع ذلك أن يباشر الخبير عمله في غياب الخصوم وأن يمنعهم كذلك من الحضور إذا كان للمنع سبب وبعد الحصول على المستندات خلال عملية التفتيش أمرا سهلا حيث يمكن التعرف عليها بالرؤية ولن يحتاج المحقق لأي مساعدة من قبل الخبراء وهذه المستندات مثل :أدلة عمل النظام ،سجلات إدارة الكمبيوتر ،وثائق البرامج السجلات صيغ مدخلات البيانات والبرامج .وكذلك صيغ مخرجات الكمبيوتر المطبوعة، ويتم التخطيط على هذه المستندات ويمكن تحديد ما إذا كانت كاملة أصلية، أو صور من خلال استجواب القائمين على حفظها.

وقد يكون التحفظ على المواد بوسائل الكمبيوتر الأخرى أمر أكثر تعقيدا مثل: الأشرطة الممغنطة، الاسطوانا، البرامج، ويحتاج إلى معونة أحد

---

(1) راجع في ذلك

Investigating computer crimes
Franklin clark den diliberto p. 147

(2) نقض مصري 1926/12/26 المحاماة س7ص789و 1927/2/8 ص8 ص1958 و1937/3/1 مجموعة القواعد القانونية جـ4 ، ص52 ، رقم 43.

الخبراء الموثوق فيهم حتى يتمكن المحقق من اللالمام بمحتويات الأشرطة أو الاسطوانات دون احداث أي تغير فيها .

وبالطبع ،فإن البحث عن المعلومات داخل جهاز الكمبيوتر ذاته يعد أمرا بالغ التعقيد ويحتاج إلى وجود خبير[1]

وأهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم المعلوماتية هي:

أولا : ما يتعلق بالوصف

أ- تركيب الحاسبات وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها بالاضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور أو السر ونظام التشفير ...إلخ .

ب- بيعة بيئة الحاسب أو الشبكةمن حيث تنظيم ،ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائط الاتصالات وتردد موجات البث وأمكنة اختزانها.

ج- الموضع المحتمل لأدلة الاثبات والشكل أو الهيئة التي تكون عليها .

د- أثر التحقيق من الوجهة الاقتصادية والمالية على المشاركين في استخدام النظام .

ثانيا : ما يتعلق بالبيان

أ- كيف يمكن عند الاقضاء عزل النظام المعلوماتي دون اتلاف الأدلة أو تدميرها أو الحاق ضرر بالأجهزة .

ب- كيف يمكن عند الاقتضاء نقل أدلة الاثبات إلى أوعية ملائمة بغير أن يلحقها تلف.

(1) راجع في ذلك :

بحث مقدم من مركز البحوث والدراسات بشرطة دبي – الإمارات العربية المتحدة بعنوان: جرائم الكمبيوتر سنة 1998 ص2

ج- كيفية تجسيد الأدلة في صورة مادية بنقلها إذا أمكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها ،مع اثبات أن المسطور على الورق مطابق للمسجل على الحاسب أو النظام أو الشبكة أو الدعامة المغنطة[1].

- الضبط في مجال الجريمة المعلوماتية

معنى الضبط وطبيعته:

يقصد بالضبط في قانون الاجراءات الجنائية، وضع اليد على شئ يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وهو من حيث طبيعته القانونية قد يكون من اجراءات الاستدلال أو التحقيق .

وتحدد طبيعته بحسب الطريقة التي يتم بها وضع اليد على الشئ المضبوط. فإذا كان الشئ وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته كان الضبط بمثابة اجراء تحقيق ،أما إذا كان الاستيلاء عليها دون الاعتداء علي حيازة قائمة فإنه يكون بمثابة اجراء استدلال .

محل الضبط :

الضبط بطبيعته ويحسب تنظيمه القانوني وغايته لا يرد إلا على الأشياء أما الأشخاص فلا يصلحون محلا للضبط بالمعنى الدقيق وإذا كان قانون الاجراءات يتحدث في بعض النصوص عن ضبط الاشخاص واحضارهم فإنه يعني القبض عليهم واحضارهم .والقبض نظام قانوني يختلف تماما عن ضبط الأشياء.

ولا يفرق القانون في مجال الضبط بين المنقول والعقار فكلاهما يمكن ضبطه كذلك فإنه يستوي أن يكون الشئ المضبوط مملوكا للمتهم أو لغيره

---

(1) انظر في ذلك :

د. هشام محمد فريد رستم، سابق الإشارة إليه ، ص41.

والقاعدة لا يرد إلا شئ مادي أما الأشياء المعنوية فلا تصلح بطبيعتها محلا للضبط والشرط اللازم لصحة الضبط أن يكون الشئ مفيدا في كشف الحقيقية فكل ما يحقق هذه الغاية يصح ضبطه .

والأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتي والتي لها قيمة خاصة في أثبات جرائم ونسبتها إل المتهم هي:

1-الورق :

كثير من الجرائم الواقعة على المال أو على جسم الإنسان تترك خلفها قدرا كبيرا من الأوراق والمستندات الرسمية منها والخاصة ،إلا أن وجود أجهزة الحاسب يجعل كثيرا من المعلومات يتم حفظها في الحاسب الآلي ،مما قلل حجم الأوراق والملفات ومع ذلك نجد أن الكثيرين يقومون بطباعة المعلومات لأغراض المراجعة، أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات موضوع الجريمة، وأجهزة الحاسب الآلي والطابعات المتطورة ذات السرعة الفائقة تطبع قدرا كبيرا من الاوراق في وقت قصير عليه يعتبر الورق من الأدلة التي ينبغي الاهتمام بها في البحث وتفتيش مسرح الجريمة. **والورق أربعة أنواع:**

أ- أوراق تحضيرية يتم اعدادها بخط اليد كمسودة أو تصور للعملية التي يتم برمجتها .
ب- أوراق تالفة تتم طباعتها للتأكد ،ومن ثم القاؤها في سلة المهملات
ج- أوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة.
د- أوراق أساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحسابات وتكون لها علاقة بالجريمة خاصة عند تقليدها أو تزوير بياناتها لتنفيذ جريمة الحاسب الآلي .

2- جهاز الحاسب الآلي وملحقاته :

وجود جهاز حاسب آلي مهم للقول بأن الجريمة جريمة حاسب آلي وأنها مرتبطة بالمكان أو الشخص الحائز على الجهاز ولأجهزة الحاسب الآلي أشكال وأحجام وألوان مختلفة، وخبير الحاسب الآلي يستطيع ان يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الالكترونية الأخرى وتحديد أسلوب التعامل معه في حالة الضبط والتحريز .

ومن السهل التعرف على جهاز الحاسب الآلي الشخصي الذي أصبح مألوفا اليوم فهو يتكون من وحدة المعالجة المركزية ، لوحة المفاتيح والشاشة ومع التطورات السريعة التي يمر بها الحاسب الآلي نجد اضافات جديدة مثل المودم والماوس والسماعات والسيرفر، وإذا كنا بصدد الحديث عن الأجهزة الكبيرة فإننا نجد أن أشكالها تتغير باستمرار خاصة من حيث الحجم والهيكل ومن الضروري اطلاع العاملين في مجال التحقيق على مختلف أشكال أجهزة الحاسب الآلي فور ظهورها.

3- أقراص الليزر :

مع أى جهاز شخصي عادي تجد قدرا كبيرا من أقراص الليزر علاوة على أن مراكز الحاسب الآلي في الشركات والبنوك تجد فيها الآلاف من الأقراص، وقد تكون على غلاف القرص بيانات توضح محتويات القرص إلا أن ذلك لا يعتد به في التحقيق الذي يتطلب بيانات دقيقة عن محتويات كل قرص وبمعرفة خبير يقدم الدليل أمام المحكمة، وقد تجد في مكان ما أقراص الليزر ولا نجد معها أجهزة حاسب آلي، ومع ذلك يعد جزءا من جريمة حاسب آلي متى كانت محتوياتها عنصرا من عناصر الجريمة.

4- الشرائط الممغنطة:

تستعمل الشرائط الممغنطة عادة للحفظ الاحتياطي وقد تكون في مكان بعيد آمن كما يقوم البعض بإيداعها في خزائن البنوك التجارية أو مراكز التوثيق الحكومية الآمنة .

5- لوحة الدوائر

6- المودم:

المودم هي الوسيلة التي تمكن أجهزة الحاسب الآلي من الاتصال مع بعضها البعض عبر خطوط الهاتف وقد تطورت المودم إلى أجهزة ارسال الفاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها وللمودم أشكال وهياكل تتطور مع تطور تقنية صناعة الحاسب الآلي .

7- الطابعات:

وللطابعات أنواع منها العادية ومنها طابعات ليزرية منها الملونة ومنها غير الملونة .

8- PEMCIA CARDS:

وتستعمل بطاقات في أجهزة الحاسب الآلي الصغيرة النوت بوك واللاب توب وهي في شكل البطاقات الائتمانية .

9- البرامج اللينة والمراشد :

المراشد المصاحبة للحاسب الآلي مفيدة في التعرف على الجهاز والبرامج المستعملة فيها.

10- البطاقات الممغنطة وبطاقات الائتمان القديمة والمواد البلاستيكية الستعملة في اعداد تلك البطاقات تعتبر قرائن للاثبات في جرائم الحاسب الآلي.

كل ذلك يعد أثرا أو جزءا من جسم الجريمة ينبغي البحث عنها وفحصها والاستفادة منها في التحقيق، علما بأن التعامل مع مثل هذه الآثار يحتاج إلى خبرة فنية في مجال الحاسب الآلي ومعرفة بالقانون وقواعد البيئة[1].



(1) راجع في ذلك :
د. محمد الأمين البشري، سابق الإشارة إليه ص33.

المبحث الثانى
معوقات جمع الأدلة فى مجال جريمة سرقة المعلومات

إن أهم ما يميز جرائم نظم المعلومات صعوبة اكتشافها واثباتها وهى صعوبة يعترف بها جميع الباحثين فى هذا المجال [1]. علاوة على ما تتميز به اجراءات جمع الأدلة فى هذا المجال من ذاتية خاصة.

وتنقسم المعوقات فى هذا الصدد إلى عدة أنواع نفصلها فيما يلى:

- معوقات خاصة بطبيعة الجريمة وأدلتها:

أولا: المعوقات الخاصة بطبيعة الجريمة (جريمة غير مرئية)

تتسم الجرائم التى تقع على الحاسبات وشبكات المعلومات بأنها غير مرئية فى العديد من حالاتها[2]. حيث لا يلاحظها المجنى عليه غالبا أو يدرك حتى بوقوعها.

---

(1) انظر في ذلك :

د. محمد زكي – الاثبات في المواد الجنائية ، ص16 ، د.محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات ، ص398 – 399 د. هدى حامد قشقوش ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25-28 أكتوبر 1993 ، منشورات دار النهضة العربية 1993 ، ص450 و476 و576. د. زكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة، 25-28 أكتوبر 1993 ، العقيد علاء الدين محمد شحاته – رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي – القاهرة 25-28 أكتوبر 1993.

(2) انظر في ذلك :

إذ تقع هذه النوعية من الجرائم في بيئة لا تعتمد التعاملات فيها أصلا على الوثائق والمستندات المكتوبة بل على نبضات اليكترونية غير مرئية لا يمكن قرائتها إلا =

واخفاء السلوك المكون لها وطمس أو تغطية نتائجها عن طريق التلاعب غير المرئى فى النبضات أو الذبذبات الالكترونية التى تسجل البيانات عن طريقها ليس مستحيلا فى الكثير من أحوالها بحكم توافر المعرفة والخبرة الفنية فى مجال الحاسبات لدى مرتكبها.[1]. اختلاس المال عن طريق التلاعب فى برامج الحاسب ومحتوياته, وغالبا ما يتم فى مخرجات الحاسب تغطيتة وستره. والتجسس على ملف البيانات كان خطأ مصدره البرامج أو الأجهزة أو نظام التشغيل أو التصميم الكلى للنظام المعلوماتى.

ونتيجة لهذه الصعوبة أصبح لإمكانية أخفاء الجريمة المعلوماتية عن طريق التلاعب فى البيانات مصطلحا يستخدم فى أبحاث علم الاجرام الأمريكية وهو (الطبيعة غير الأولية لمخرجات الحاسب المطبوعة)[1] Second-hand Nature computer printouts.

=بواسطة الحاسب الآلي والبيانات التي يمكن استخدامها كادلة ضد الفاعل يمكن في أقل من الثانية العبث به أو محوها بالكامل لذا فإن للمصادفة وسوء الحظ دورا في اكتشافها يفوق دور اساليب التدقيق والرقابة ومعظم مرتكبيها اللذين تم ضبطهم وفقا لما لاحظه أحد الخبراء، إما أنهم قد تصروفوا بغباء أو أنهم لم يستخدموا الأنظمة المعلوماتية بمهارة : انظر :

John Eaton and Jermy smithers, this is it. Amangagrs Guide to information technology , London, Philip Allan , 1982p.263

مشار إليه د. هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت في الفترة من 1-3 مايو 2000 بجامعة الإمارات العربية المتحدة بعنوان الجرائم المعلوماتية).

(1) انظر في ذلك :

Jay , J. Becker the Trial of computer crime (1980), 2 computer Law , Journal 441

مشار إليه الدكتور هشام محمد فريد رستم ، سابق الإشارة إليه.

ثانيا : معوقات خاصة بأدلة الجريمة

(أ) انعدام الدليل المرئى:

يلاحظ أن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التى تقع عليها أو بواسطتها ما هى إلا بيانات غير مرئية لا نفصح عن شخصية معينة وهذه البيانات مسجلة الكترونيا بكثافة بالغة وبصورة مرمزة[1]. غالبا على دعائم أو وسائط للتخزين ضوئية كانت أو ممغنطة لا يمكن للإنسان قراءتها وإن كانت قابلة للقراءة من قبل الآلة نفسها ولا يترك التعديل أو التلاعب فيها أى أثر مما يقطع أى صلة بين المجرم وجريمته ويعوق أو يحول دون كشف شخصيته[2].وكشف وتجميع أدلة بهذا الشكل لإثبات وقوع الجريمة والتعرف على مرتكبيها هو أحد أبرز المشاكل التى يمكن أن تواجه جهات التحرى والملاحقة.

وتبدو هذه المشكلة بشكل عام فى سائر مجالات التخزين والمعالجة الآلية للبيانات حيث تنتفى غالبا قدرة ممثلى الجهات المختصة على أن يتولوا بطريقة مباشرة فحص واختبار البيانات المشتبه فيها وتزداد جسامة هذه المشكلة بوجه خاص فى حالة التلاعب فى برامج الحاسب نظرا لتطلب الفحص الكامل للبرنامج واكتشاف التعليمات غير المشروعة المخفية داخله قدرا كبيرا من الوقت والعمل,وغالبا ما لا يكون له من حيث التكلفة الاقتصادية مبررا[3].

---

(1) Les dificultes techniques sont liees aux methoded de cryptologie employees sur le reseua .
La criminamite informatique sur linternet , p. 58

(2) انظر في ذلك :

Ulrich , sieber, ibid, p. 140

(3) راجع في ذلك :

وتدليلا على تأثير غياب الدليل المرئي في إعاقة اجراءات الضبط وملاحقة مرتكبي

(ب) سهولة محو الدليل أو تدميره فى فترة زمنية يسيرة:

من الصعوبات التى يمكن أن تعترض عملية الاثبات فى مجال جرائم نظم المعلومات سهولة محو الجانى أو تدميره لأدلة الإدانة فى فترة زمنية وجيزة فضلا عن سهولة تنصله من هذا العمل بإرجاعه إلى خطأ فى نظام الحاسب أو الشبكة أو فى الأجهزة ومن الأمثلة الواقعية قيام أحد مهربى الأسلحة بإدخال تعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه فى تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر إلى الحاسب من خلال لوحة مفاتيحه بالنسخ أو الطبع أو تدمير البانات كلها.

=

الجرائم التي تقع في مجال تكنولوجيا المعلومات يشير الأستاذ sieber إلى حالة واقعية شهدتها المانيا الاتحادية سابقا عام 1971 تلخص وقائعها في اكتشاف شركة طلبياتها بريدية mail order firm سرقة أشرطة ممغنطة تخصها تحوي 300000 عنوانا لعملاتها وتمكنها من استصدار أمر من المحكمة . معروف باسم وقف الأعمال injuction باستعادة كل العناوين من شركة منافسة كانت قد حصلت على هذه العناوين من مرتكبي السرقة ، وتنفيذا لهذاالأمر سمحت الشركة المنافسة لمساعدة مأمور التنفيذ بدخول مقرها ومركز الحاسب الخاص بها، حيث وجد نفسه أمام كم هائل من الأشرطة والاقراص الممغنطة التي لا يدري عنها شيئا أو يعرف محتوياتها أو لديه القدرة على فحصها ومعرفة مضمونها، مما اضطر إلى مغادرة مركز حاسب الشركة المنافسة خالي الوفاض ومع أن الشركة المناسبة قامت من تلقاء نفسها بعد ذلك بعدة أيام بتسليم بيانات العناوين إلى الشركة المجني عليه إلا أنه من الوارد بالتأكيد - أن تكون الاشرطة المعنية قد تم استنساخها قبل تسليمها ، وهو ما يكون قد افقد امر المحكمة جدواها.
راجع Ulrich siber , ibid ,p. 140

ومع أن تعديل برمجة نظام تشغيل الحاسب كان قد أجرى خصيصا بواسطة الفاعل للحيلولة دون نجاح أجهزة الملاحقة فى اجراءات المتوقعة للبحث عن الأدلة وضبطها إلا أنه لم يفلح فى تحقيق هذا الهدف نتيجة لتوقع المتخصصين لمعالجة البيانات بالجهاز المركزى لمكافحة الغش المعلوماتى بالنمسا بأن شئ ما فى نظام تشغيل حاسب الفاعل قد جرى تغييره وقيامهم بناءا على ذلك باستنساخ الأقراص الممغنطة المضبوطة عن طريق أنظمة حاسباتهم[1].

وفى حالة أخرى شهدتها المانيا الاتحادية سابقا أدخل الجناة فى نظام الحاسب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها ومن شأنها محو هذه البيانات بالكامل بواسطة مجال مهربائى وذلك إذا ما تم اختراقه من قبل شخص غير مرخص له[2].

(جـ) صعوبة الوصول إلى الدليل:

تحاط البيانات المخزنة الكترونيا أو المنقولة عبر شبكات الاتصال بجدار من الحماية الفنية لإعاقة محاولة الوصول غير المشروعة إليها للاطلاع عليها أو استنساخها[3].. كذلك يمكن للمجرم المعلوماتى أن يزيد من صعوبة

---

(1) راجع في ذلك :

د. هشام محمد فريد رستم ، سابق الإشارة إليه، ص35-36

(2) راجع في ذلك :

Ulrich sieber, ibid, p. 141

(3) تواجه عملية جمع الأدلة الاليكترونية واستعمالها بعض التحديات الرئيسية major challenges ومنها :

- صعوبة الوصول إلى الملفات المحذوفة أو المخبأة أو المحمية بموجب كلمات مرور داخل النظم الضخمة المرتبطة من خلال الشبكات.
- صعوبة استعادة البيانات من بعض الوسائل أو الوسائط القديمة.

عملية التفتيش التى قد تباشر للحصول على الأدلة التى تدينه عن طريق مجموعة من التدابير الأمنية كاستخدام كلمة السر للوصول إليها أو دس تعليمات خفية بينها أو ترميزها لإعاقة أو منع الاطلاع عليها أو ضبطها . لذا فأن استخدام تقنيات التشفير لهذا الغرض يعد إحدى العقبات الكبرى التى تعوق رقابة البيانات المخزنة أو المنقولة عبر حدود الدولة والتى تقلل من قدرة جهات التحرى والتحقيق والملاحقة على الاطلاع عليها الأمر الذى يجعل حماية حرمة البيانات الشخصية المخزنة فى مراكز الحاسبات والشبكات أو المتعلقة بالأسرار التجارية العادية والالكترونية أو بتدابير الأمن والدفاع أمر بالغ الصعوبة(1).

وتصطدم عقبة الوصول إلى الدليل المعلوماتى بمشكلة اجرائية تتعلق بمدى سريان القيود الخاصة بضبط الأوراق على ضبط محتوى نظام المعالجة الآلية للبيانات والمحمى فنيا فى مواجهة الاطلاع غير المسموح به حيث يحظر قانون الاجراءات الجنائية المصرية والإماراتى بمقتضى المادتين

=

- صعوبة العثور على الملفات او السجلات المحورية من بين المجالات الشاسعة للبيانات (مثال : سجلات البريد الالكتروني)
- صعوبة تحليل صحة الملفات - ومعرفة ما إذا كان قد تم تعديلها او محوها :
- راجع في ذلك :

Linda volonino ph. D.ibid., p.14

(1) انظر في ذلك :

يشير الأستاذ sieber بأن مشاكل عديدة لا يستهان بها قد نجمت من استخدام الجناة في بعض الجرائم المعلوماتية التي وقعت بالمانيا الاتحادية سابقا لتقنيات التشفير أو الترميز لإعاقة اكتشاف أو الوصول إلى أدلة تدينهم وبوجه خاص في مجال وسائل التخزين التي يكون صعبها ضبطها.

راجع في ذلك : Ulrich Sieber Ibid, p. 141

52, 58 على التوالى[1]. اطلاع مأمور الضبط القضائي على الأوراق المختومة أو المغلقة[2]. الموجودة فى منزل المتهم أثناء تفتيشه[3].وعلة ذلك الحفاظ على الآثار التى تتضمنها الأوراق وهنا يثور تساؤل عما إذا كان حكم هاتين المادتين واجب الإتباع بالنسبة لإطلاع مأمور الضبط القضائى على محتوى نظام المعالجة الآلية للبيانات من عدمه وذلك فى حالة ما إذا كان محاطا بجدار من الحماية الفنية تعوق الاطلاع عليه. ونبادر بالإيجاب على هذا التساؤل استنادا إلى سببين:

الأول: أن السبب الذى من أجله تم تقرير هذا الحكم بالنسبة للأوراق المختومة أو المغلقة يتوافر أيضا بالنسبة لمحتوى نظام المعالجة الآلية للبيانات المحمى فنيا ضد الإطلاع غير المسموح به.

فحظر المشرع اطلاع مأمور الضبط القضائى على هذه الأوراق مما هو لمظنة أن الغلق أو التغليف يضفى عليها مزيدا من السرية ويفصح عن رغبة صاحبها فى عدم اطلاع الغير على مضمونها بغير إذنه وهو ما يتحقق فى البيانات المخزنة أو المنقولة عبر نظام أو شبكة حاسب إذا كانت محمية فنيا ضد الاطلاع غير المسموح به . فمحتوى النظام لا يكون بذلك مكشوفا بل

(1) تنص المادة الأولى منهما على أنه " إذا وجدت في منزل المتهم أوراق مختومة أو مغلقة بأية طريقة فلا تجوز لمأمور الضبط القضائي أن يفضها ، وبذات الصياغة تقريبا يسري نص المادة 58 أ.ج. إماراتي .

(2) فإذا كانت ظاهرا أن التغليف لا ينطوي وإنما يحوي جسما صلبا، فإنه يجوز لمأمور الضبط القضائي فض الغلاف لفحص محتوياته نقض مصري 24 يونية 1958 ، مجموعة أحكام النقض س9 رقم 180 ص716.

(3) قضى في مصر بعدم دستورية المادة 47 من قانون الإجراءات الجنائية المصري في 2 يونيه 1984 ومن ثم لم يعد هناك مجال لتطبيق نص المادة 52 من هذا القانون في حالة التلبس بالجريمة.

محجوبا عن الغير حيث لا يتاح الوصول والاطلاع عليه بغير معرفة طريق ومفاتيح وكود التشغيل [1].

الثانى: أن المادة 52 اجراءات مصرى (58 اجراءات اماراتى) تضع قاعدة عامة لضمان الأسرار التى تحتويها سائر وسائط وأوعية حفظ وتخزين ونقل المعلومات سواء ما كان منها تقليديا كالأوراق أو مستحدثا كالأقراص المرنة والأشرطة الممغنطة والذكرات الداخلية للحاسبات وشبكات المعلومات المحلية والإقليمية والعالمية.

والجدير بالإشارة إليه أن كلا من التشريعين الإجرائيين المصرى والاماراتى لا ينفردا بهذه النتيجة بل يشاركهما فيها العديد من القوانين ومنها على سبيل المثال قانون الاجراءات الجنائية الالمانى , فطبقا للمادة 110 منه تقتصر سلطة الاطلاع على مخرجات الحاسب وغيرها من دعائم البيانات على المدعى العام وحده , ولا يكون لضباط الشرطة حق الاطلاع على البيانات عن طريق تشغيل البرامج أو الاطلاع على ملفات البيانات المخزنة داخل الحاسب بغير إذن من له حق التصرف فيها , ومالهم قانونا هو فحص دعائم البيانات عن طريق النظر فحسب دون استخدام مساعدات فنية [2].

(د) افتقاد الآثار المؤدية إلى الدليل:

يحدث فى بعض الأحيان إدخال البيانات مباشرة فى نظام الحاسب دون تطلب وجود وثائق معاونة (وثائق خاصة بالإدخال) كما هو الحال فى بعض

(1) راجع في ذلك :

د. هشام محمد فريد رستم، سابق الإشارة إليه ص34.

(2) انظر في ذلك :

Manfred Mothren schlager, computer crimes and other crimes against information technology in Bermany , rev, inter, D.P. leret 2e trimesters 1993,p.351

نظم العمليات المباشرة التى تقوم على استبدال الإذن الكتابى لإدخال البيانات بإجراءات أخرى تعتمد على ضوابط للإذن متضمنة فى برنامج الحاسب (مثل المصادقة على الحد الأقصى للإئتمان وفى مجال العمليات المالية قد يباشر الحاسب بعض العمليات المحاسبية بغير الحاجة إلى ادخال كما هو الحال لإحتساب الفائدة على الإيداعات البنكية وقيدها آليا بأرصدة حسابات العملاء على أساس الشروط المتفق عليها مسبقا والموجودة فى برنامج الحاسب.

ويكون من السهل فى كل من هذين النوعين من العمليات ارتكاب بعض أنواع من الجرائم كاختلاس المال والتزوير بإدخال بيانات غير معتمدة فى نظام الحاسب أو تعديل برامجه أو البيانات المخزنة داخله دون أن يترتب على ذلك أى أثر يشير ألى حدوث هذا الادخال أو التعديل . لذا يتعين على المحقق إزاء صعوبة الوصول إلى مرتكبى الجرائم فى كلا هذين النوعين من العمليات وعدم ترك التغيرات فى البرامج أو البيانات آثار كتلك التى يخلفها التزوير المادى فى المحررات التقليدية[1]. أن يسعى لتحديد دائرة الأشخاص القائمين أو المتصلين فى عمليات ادخال ومعالجة البيانات وغيرها من عمليات التسجيل[2]. مع الاستفادة من ضوابط الرقابة التى تباشر فى النظام المعلوماتى على الإدخال والمعالجة اضافة إلى تتبع الأموال المختلفة إن وجدت باعتبارها محصلة الجريمة التى يستولى عليها المجرم فى نهاية الأمر[3].

---

(1) راجع في ذلك :

Jack Bologena corporate faraud : the Basice of prevention and detection , Butterworth publishers 1984,p.75

(2) راجع في ذلك :

J.Tappolet , La fracuc infromatieque, rev, int , crim poltech 1988,p.351

(3) راجع في ذلك :

د. هشام محمد فريد رستم ، سابق الإشارة إليه ص31.

المعوقات الخاصة بالعامل البشرى

- ويتعدد هذا النوع من المعوقات على النحو التالى:

1- مكان ارتكاب الجريمة:

يتم ارتكاب جريمة الحاسب الآلى عادة عن بعد حيث لا يتواجد الفاعل على مسرح الجريمة ومن ثم تتباعد المسافات بين الفعل (من خلال حاسب الفاعل) و النتيجة (المعطيات محل الاعتداء) وهذه المسافات لا تقف عند حدود الدولة بل قد تمتد إلى النطاق الإقليمى لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها[1].

فقد أعلنت السلطات البريطانية أن أكثر من عشرة ألاف اسطوانة تعليمية عن الإيدز قد أدخلت إلى المستشفيات فى كل من بريطانيا والسويد والدنمارك والنرويج.

وقد اكتشفت أجهزة البيانات أنها مصابة بفيروس "نورجان " وهو فيروس يؤدى إلى تخريب أجهزة الكمبيوتر الشخصى واتلاف البرامج التى تعمل عليع وفى غضون ذلك. بدأت شرطة سكوتلانديارد تحقيقات واسعة النطاق فى هذه القضية باعتبارها جريمة تخريب وقد أثبتت التحقيقات مايلى:

(أ) أن هذه الاسطوانة وصلت إلى الأشخاص بالبريد من مصادر مختلفة بهدف تخريب البرامج المرسلة إليهم وأن أسماء الذين وجهت لهم الاسطوانات يبلغ عددهم نحو سبعة آلاف شخص قد تم بيعها إلى شركة تدعى " كيتيما " وهى مؤسسة تخص رجل أعمال كينى " يدعى كيتيما"

(1) راجع في ذلك : د. أسامة محمد محي الدين عوض، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25-28 أكتوبر 1993.

وقد اتضح أن قائمة الأسماء التى أحضرت معه خلال زيارته لبريطانيا فى الفترة من 31 أكتوبر حتى 30 نوفمبر 1989 ولكنه لم يستدل له على عنوان.

(ب) أن عددا من هذه الاسطوانات ظهرت فى كاليفونيا وفى بلجيكا وزيمبابوى.

(ج) الرسائل أرســـلت مع رسائل معنوية بـ "معلومات عن الإيدز " لكن تبين أنها تحتوى على فيروس نورجان الذى يهاجم أجهزة الحاسب الشخصى من نوع I . B . M والمتوافقة معه.

(د) تسأل الرسالة المرفقة مع الاسطوانة عن رسوم ملكية للبرنامج بمقدار 189 دولار أو 378 دولارا حسب الطلب وإرسال الرد إلى عنوان فى بنما ولكن تبين أن معظم الرسائل أرسلت من لندن وبالتحرى تبين عدم وجود شركة بهذا الاسم ولا يوجد لها صندوق بريد فى بنما . بينما تبين أن مرسل الرسالة استخدام الاسم الأول من إحدى شركات البرامج الأمريكية العاملة فى بنما والتى أكدت عدم مسئوليتها عما حدث.

(و) تحذر الرسالة من أنه فى حالة عدم دفع الرسوم سيستخدم المرسل برنامجا لتخريب المعلومات ووقف جهاز الكمبيوتر بشكل تلقائى ولكن ما أثار الانتباه إلى هذه القضية حدث خلال تحميل الاسطوانة وفقا لما قاله "جرسيرست" خبير الفيروسات ومستشار التطبيقات البريطانى [1].

2- نقص خبرة الشرطة وجهات لادعاء والقضاء:

يتطلب كشف جرائم الكمبيوتر والوصول إلى مرتكبيها وملاحقتهم قضائيا استراتيجيات خاصة تتعلق بإكسابهم مهارات خاصة وعلى نحو يساعدهم على

(1) راجع في ذلك :

د. أسامة محمد محي الدين عوض ، سابق الإشارة غليه ، ص430 - 431

مواجهة تقنيات الحاسب الآلى المتطورة وتقنيات التلاعب به, حيث تنعقد وتتنوع التقنيات المرتبة بوسائل ارتكابها[1].

لذا يجب استخدام أساليب وتقنيات تحقيق جديدة ومبتكرة لتحديد نوعية الجريمة المرتكبة وشخصية مرتكبها وكيفية ارتكابها مع الاستعانة بوسائل جديدة أيضا لضبط الجانى والحصول على أدلة ادانته.

إذ من المتصور أن يجد مأمورى الضبط القضائى أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والاجراءات التقليدية مع هذه النوعة من الجرائم[2]. ومما يزيد من صعوبة هذا الأمر افتقار أنظمة الحاسبات وشبكات المعلومات فى البدايات الأولى لاستخدامها لأساليب الرقابة وضوابط التدقيق والمراجعة على العمليات والتطبيقات وعدم تزويدها بوسائل فنية لاكتشاف وتتبع مسار العمليات[3] , فضلا عن ما تصادفه هذه الجهات من صعوبات فى التحرى عن جرائم الحاسب عابرة الحدود لا سيما بعد انتشار استخدام شبكة المعلومات العالمية.

---

(1) انظر في ذلك :

Donn, B., Parkar, vulnerabilities of EFT systm to intentionally causes losses in computers and Banking electronic funds transfer system and public poliecy edited by Kent w.colton and Keneth L. Kraemer, plenum press 1980,p. 97

(2) جاء بتوصية المجلس الأوروبي رقم (95) 13 في 11 سبتمبر 1995 في شأن مشاكل الاجراءات الجنائية المتعلقة بتكنولوجيا المعلومات ضرورة تشكيل وحدات خاصة لمكافحة جرائم الحاسب وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.

(3) راجع في ذلك :

Bernard P. zajac Jr. police responses to computer crime in the united states the computer law and security report July – auyg 1985,pp.16-17

وكثيرا ما تفشل أجهزة الشرطة فى تقدير أهمية الجريمة المعلوماتية نظرا لنقص الخبرة والتدريب[1]. وللسبب ذاته أيضا كثيرا ما تفشل جهات التحقيق فى جمع أدله جرائم الحاسب الآلى مثل مخرجات الحاسب وقوائم التشغيل , بل أن المحقق كما هو الحال أحيانا فى بعض الجرائم الأخرى قد يدمر الدليل بمحوه الاسطوانة الصلبة من خطأ منه أو أهمال أو بالتعامل مع الأقراص المرنة أو بالتعامل المتسرع أو الخاطئ مع الأدلة[2].

---

(1) لقد علمت أن شابا طلب نسخة اسطوانة كمبيوتر وقام بتصوير البطاقة الملصقة عليها ثم قام بوضع الاسطوانة على السطح الزجاجي لآلة التصوير إلا أن الاستاتيكية التي نشأت عندما عملة الآلة أدت إلى مسح وإمالة كافة المعلومات المسجلة على الاسطوانة وهناك حالة أخرى حيث قام رجال الشرطة بوضع حقيبة كاملة تحتوي علىاسطوانات الكمبيوتر المصادرة وذلك في صندوق السيارة بالقرب من جهاز الإرسال والاستقبال اللاسلكي فكانت النتيجة أن الإشارات الكهربائية القوية تسبب في تدميرها جميعا.
انظر في ذلك :

Burici sterling ibid, p. 208

وصرح مكتب التحقيقات الفيدرالي بأن خبارته لم يتمكنوا من تحديد ما إذا كان الحدث قد وقع بسبب عطل فني أو هجوم ماكر وقد حجب الموقع الخاص بشركة السمسمرة الوطنية والذي يرتاده 200 ألف عميل لمدة تفوق الساعة – حاول خلالها مهندسوا الشركة الدفاع عن النظام ضد ما رأوا أنه هجوم . فقد لاحظوا مسئولوا الشركة أن الموقع كان يعمل ببطء شديد عند افتتاح السوق وهو الأمر الذي أدى إلى انخفاض إمكانية الوصول إليه إلى 50%.
راجع في ذلك

D. voloninalinu ibid, p. 6

(2) انظر في ذلك :

Richard totta and antong hardcastle, computer related crime in information technology the law edited by chris Edwards and Nigel savage Macmillan publisher 1986,p.201

تكمن المشكلة فيما يقوم به رجال الشرطة حين يستخدم الكمبيوتر كأداة لارتكاب الجريمة فى المعوقات التى يمكن أن تواجه فى هذا المجال وهى:

- اما تجاهل هذا الدليل تماما.
- اما محاولة فحص هذا الدليل بدون أية مهارات فى مجال الكمبيوتر .
- اما حمل المشتبه فيه على استعادة معلومات من الكمبيوتر. ثم بعد ذلك عدم مصادرة نظام الكمبيوتر حيث أن الشهادة التى يدلى بها تصبح حرجة فى مواجهة المعلومات المستمدة من الكمبيوتر.
- واما مصادر جهازالكمبيوتر بدون معرفة ما يوجد فيه من معلومات وبالتالى زيادة الفرصة فى فقد هذه المعلومات.

3- إحجام المجنى عليهم عن التبليغ:

ويعد هذا الأمر على قدر من الصعوبة لا فى مجال اكتشاف واثبات جرائم الحاسب بل وفى دراسة هذه الظاهرة برمتها وهو ما يعبر عنه بالرقم الأسود[1]. لجرائم الحاسب .

(1) ويلاحظ في هذا الشأن أن المشرع الإماراتي جعل الإبلاغ عن الجرائم الزامي كقاعدة عامة وإلا تعرض المخالف للجزاء الجنائي، إذ أوجب لمقتضي المادة (37) من قانون الإجراءات الجزائية رقم 35 لسنة 1992 ، وعلى كل من علم بوقوع جريمة مما يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب أن يبلغ النيابة العامة أو مأموري الضبط القضائي عنها ، ونص في المادة (38) من القانون ذاته على أنه يجب على كل من علم من الموظفين العمومين أو المكلفين بخدمة عامة أثناء تأدية عمله أو بسبب تأديته بوقوع جريمة من الجرائم التي يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب. أن يبلغ عنها فورا النيابة العامة أو أقرب مأموري الضبط القضائي ورصد مخالفة هذاالواجب عقوبة جنائية ينصه في الفقرة الثانية من المادة (272) من قانون العقوبات الاتحادي على " أن ... يعاقب بالغرامة كل موظف غير مكلف بالبحث عن الجرائم ا أو ضبطها أعمل أو أرجأ إبلاغ السلطة المختصة بجريمة علم بها في أثناء أو بسبب تأديته وظيفته ولا عقاب إذا كان رفع

وفى هذا الشأن يحدثنا Beter swift يعتقد اتحاد الصناعة البريطانى confederation of britich industry»» أن العديد من الشركات تحرج من الاعتراف بأنها تعرضت للسلب حسب تعبيره من قبل مجرمى التقنية العالمية فبدلا من استدعاء الشرطة والاعتراف بأنهم ضحايا جرائم السرقة فإنهم يخلدون إلى الصمت[1].

ويلاحظ أن العديد من ضحايا جرائم الحاسب لا يقفون عن حد عدم الابلاغ عن الجريمة بل أنهم يرفضون أى تعاون مع الجهات الأمنية خشية معرفة العامة بوقوع الجريمة ويسعون بدلا من ذلك إلى محاولة تجاوز أثارها حتى لوكانت الوسيلة هى مكافأة المجرم ونذكر على سبيل المثال بنك Marchant bank city فى انجلترا لنقل 8 مليون جنيه استرلينى من أحد أرصدته إلى رقم حساب فى سويسرا وقد تم القبض على الفاعل أثناء محاولته سحب المبلغ المذكور ولكن بدلا من أن يقوم البنك بتحريك الدعوى الجنائية ضده فقد قام بدفع مبلغ 1 مليون جنيه استرلينى له بشرط عدم اعلام الآخرين عن جريمته واخطار البنك بالألية التى نجح من خلالها باختراق نظام الأمن الخاص بحاسب البنك الرئيسى[2].

=

الدعوى .. معلقا على شكوى ... كما جاءت المادة (274) من ذات القانون لتقضي بأن يعاقب بغرامة لا تجاوز ألف درهم كل من علم بوقوع جريمة وامتنع عن إبلاغ ذلك إلى السلطات المختصة، ويجوز الإعفاء من هذه العقوبة إذا كان من امتنع عن الإبلاغ زوجا لمرتكب الجريمة أو من أصوله أو فروعه أو أخوته أو اخوانه أو من هم منزلة هؤلاء نم الأقرباء بحكم المصاهرة،

(1) انظر في ذلك :

Peter swift Hackmun – menace of the key board criminal brithish telecom world mag half of sep. 1989,p.13-14

(2) راجع في ذلك :

Peter swift Hackan , ibid , p. 3

وفى دراسة أجريت عام 1980 فى فرنسا أشارت النتائج إلى أن جرائم الحاسب التى تم الابلاغ عنها للسلطات الخاصة بلغت 15٪ من مجموع الجرائم وأن ادلة الادانة لم تتوافر إلا لنسبة تقدر بحوالى خمس النسبة المتقدمة أى ما يعادل حوالى 3٪من مجموع جرائم الحاسب المرتكبة.

كما تؤكد دراسة حديثة أجريت فى الولايات المتحدة الامريكية أن الرقم الأسود لجرائم الحاسب يميل إلى الارتفاع فإستنادا إلى تحليل الباحثين وفى ضوء تقارير جمعيات صانعى الحاسبات يظهر أن الرقم الأسود ما يقارب نسبة 60٪ من جرائم الحاسب[1].

4- دور الخبراء فى فحص البيانات:

يشكل الكم الهائل للبيانات التى يتم تداولها من خلال الأنظمة المعلوماتية أحد مصادر الصعوبات التى تعوق تحقيق الجرائم التى تقع عليها أو بواسطتها والدليل على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات والتى قد لا تثبت كلها تقريبا شيئا على الاطلاق. ويسلك المحقق غير المدرب لمواجهة هذه الصعوبة أحد سبيلين:

اما حجز البيانات الالكترونية بقدر يفوق القدرة البشرية على مراجعتها أو الغاضى عن هذه البيانات كلها على أمل الحصول على اعتراف بالجريمة من المتهم[2].

---

(1) راجع في ذلك :

يونس خليل عرب مصطفى جرائم الحاسب - دراسة مقارنة رسالة ماجستير - مقدمة إلى كلية الدراسات العليا الجامعة الأردنية ، 1994 ، ص73

(2) راجع في ذلك :

د. هشام محمد فريد رستم سابق الإشارة إليه ، ص37

الواقع أنه بالامكان مواجهة هذة الصعوبة عن طريق أحد أمرين:

أ- الاستعانة بالخبرة الفنية لتحديد ما يجب دون سواه البحث عنه للإطلاع علية وضبطه واستعانة الجهات القائمة بالتحرى والتحقيق , والحكم بالخبراء حين تتعامل مع الجرائم التى تقع فى مجال تكنولوجيا المعلومات تكاد تكون ضروره لاغنى عنها نظرا للطابع الفنى الخاص لأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء ونجاح هذه الجهات فى أداء رسالتها يتوقف إلى حد كبير علاوة على حسن إختيار الخبير على نجاحه فى المهمة التى عهد إليه بأدائها وموضوع هذه المهمة وان كان يمكن للخبير نفسه أن يحدده إلا أن ذلك ليس مرغوبا فيه تجنبا لهيمنة دور الخبير على العملية الاثباتية وطغيانه على دور المحقق أو القاضى.

ب- الاستعانة بما تتيحه نظم المعالجة الآلية للبيانات من أساليب للتدقيق والفحص المنظم أو المنهجى ونظم ووسائل الإختبار والمراجعة.

• المعوقات الخاصة بالتنسيق الدولى فى مجال جمع الأدلة

من خصائص جرائم الحاسب إنها جرائم عابرة للحدود الوطنية أو الإقليمية أو القارية وأن مواجهتها على نحو مؤثر يتطلب العمل من خلال محورين:

الأول: سن النصوص الجنائية الموضوعية على الصعيد الوطنى لتجريم صورها المختلفة والعقاب عليها إضافة إلى سن قواعد جنائية اجرائية تتلائم مع خصائصها وطبيعتها المميزة وثانيهما:خلق وتطوير وإنماء العمل الدولى المشترك لمواجهة هذه الظاهرة من خلال وضع حلول للمشاكل التى تحد من فاعلى مكافحتها سواء المشاكل الناجمة عن تطبيق القواعد الموضوعة أو القواعد الاجرائية عل هذا النمط المستحدث من الجرائم.

وهناك عقبات عديدة تقف بمثابة حجر عثره من أجل التنسيق الدولى فى مكافحة جرائم سرقة المعلومات وأبرزها ما يلى:

1- عدم وجود مفهوم عام مشترك بين الدول حتى الآن حول نمازج النشاط المكون للجريمة المتعلقة للحاسب الآلى .

2- عدم وجود تعريف قانونى موحد للنشاط الاجرامى المتعلق بهذا النوع من الاجرام.

3- إختلاف مفهوم الجريمة لإختلاف التقاليد القانونية وفلسفة النظم القانونية المختلفة.

4- انعدام التنسيق بين قوانين الاجراءات الجنائية للدول المختلفة فيما يتعلق بالتحرى والتحقيق فى الجريمة المعلماتية.

5- تعقد المشاكل القانونية والفنية الخاصة بتفتيش نظم المعلومات خارج حدود الدولة أو ضبط معلومات مخزنة فيه أو الأمر بتسليمها.

6- عدم وجود معاهدات للتسليم أو للتعاون الثنائى أو الجماعى بين الدول تسمح بالتعاون الدولى أو عدم كفايتها إن وجدت لمواجهة المتطلبات الخاصة للجرائم المعلوماتية وسرعة التحريات فيها[1].

---

(1) لمواجهة هذه المشكلات أو بعضها، ناشد مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين والذي عقد في هافانا عام 1990 في قراره المتعلق بالجرائم ذات الصلة بالحاسب، الدول الأعضاء أن تكثف جهودها كي تكافح بمزيد من الفعاليات عمليات إساءة استعمال الحاسب التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني بما في ذلك النظر إذا دعت الضرورة في أ – تحديث القوانين والإجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل

1- ضمان أن الجزاءات والقوانين الراهنة بشأن سلطات التحقيق وقبول الأدلة في الاجراءات لاقضائية تنطبق على نحو ملائم وإدخال تغييرات مناسبة عليها إذا دعت الضرورة لذلك .

=

2- النص على جرائم وجزاءات اجراءات تتعلق بالتحقيق والأدلة حيث تدعو الضرورة إلى ذلك للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرمي في حالة عدم وجود قوانين تنطبق على نحو ملائم. كما حث المؤتمر كذلك الدول الاعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالحاسبات بما في ذلك دخولها ، حسب الاقتضاء أطرافا في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدات في المسائل الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب وتصح القرار ذاته الدول الأعضاء بالعمل على أن تكون تشريعاتها المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية منطبقة انطباقا كافيا على الأشكال الجدية للإجرام مثل الجرائم ذات الصلة بالحاسب وإن تتخذ خطوات محددة. حسب الاقتضاء من أجل تحقيق هذا الهدف وذلك بالإضافة إلى توصيات أخرى وقد يكون ملائمات كخطوة تعزز مسار التعاون الفعال وتكمل ما اتخذه مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين في هذا لاشأن من قرارات أن يسفر بحث مؤتمرات الأمم المتحدة لموضوع الجرائم ذات الصلة بالحاسب عن فتح آفاق جديدة للتعاوةن الدولي في هذا المضمار لا سيما فيما يتعلق بوضع أو تطوير أ - معايير دولية لأمن المعالجة الآلية للبيانات ب - تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود أو ذات الطبيعة الدولية جـ - اتفاقيات دولية تنطوي على نصوص تنظم اجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت نفسه لحقوق وحرياتهم وسيادة الدول.

راجع في ذلك :

د. هشام محمد فريد رستم سابق الإشارة، ص 49.

المبحث الثالث

التعاون الدولي في مجال مكافحة الجريمة المعلوماتية

أصبح لكل شخص يعيش في المجتمع الحق بالاتصال بغيره وتبادل المنافع المعنوية والمادية معه ليس فقط داخل دولته بل كذلك خارجها مع أبناء الدول الأخرى .

وإذا كانت الدول قد استطاعت الحد من ذلك الاتصال والتبادل في أوقات مضت تحت ستار حماية متطلبات أمنها القومي والاقتصادي إذ أنها لم تعد كذلك في ظل عصر السماوات المفتوحة بفعل تقدم وسائل الاتصال عبر الأقمار الصناعية[1] ووسائط نقل الأخبار المعلوماتية عبر الأثير والموجات الكهرومغناطيسية لدرجة يمكن القول معها أن سيادة الدولة الإقليمية قد انحسرت عن الإقليم الفضائي أو الهوائي واقتصرت على إقليمها الأرضي والمائي فقط [2] .

وقد كرست الأعمال القانونية الدولية حق الاتصال والحصول على المعلومات وتداولها ،وأكدت على أهمية ضمان ممارسته[3]

فقد نص القرار 59 الصادر عن الأمم المتحدة في 14 ديسمبر 1946 على أن "حرية الاستعلام هي حق أساسي للإنسان، وهي حجر الزاوية لكل

---

(1) راجع في ذلك :

Ravillon (Hume) les telecommunications par sateliet aspects juridiques Paris , ed, lifec 1997,

Mateesco – Matte (N) droit aerospatical les telcomunnications par natellites Pars , 1982

(2) راجع في ذلك

Park 9K-G) la protection de la souverainet aerienne Paris, 1977

(3) راجع في ذلك :

Pinto " la Liberte d'infromation ed d'opinion en droit international , paris , L.G.D.J. 1984

الحريات التي كرست الأمم المتحدة نفسها للدفاع عنها،وحرية الاستعلام تشمل جمع ونقل ونشر المعلومات في كل دون عقبات ".

كما نصت المادة 19 من الاعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة في 10 ديسمبر 1948 على أن "لكل فرد الحق في حرية الرأي والتعبير ويشمل هذا الحق حرية اعتناق الآراء دون تدخل واستقاء وتلقي وإذاعة الأنباء والأفكار دون تقيد بالحدود الجغرافية وبأية وسيلة كانت "

وأخيرا نصت المادة 19 من العهد الدولي للحقوق المدنية والسياسية الصادر عن الأمم المتحدة في 16 ديسمبر 1966 على أن "2- لكل فرد الحق في حرية التعبير وهذا الحق يشمل حرية البحث عن المعلومات أو الأفكار من أي نوع واستلامها ونقلها بغض النظر عن الحدود، وذلك إما شفاهة أو كتابة أو طباعة ،وسواء كان ذلك في قالب فني أو بأية وسيلة أخرى يختارها ".

وتنشأ ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات على وجه الخصوص من سهولة حركة المعلومات في أنظمة تقنية المعلومات حيث يرجع لهذه السهولة في حركة المعلومات بأنه بالامكان ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة بينما يتحقق نجاح هذا النشاط الاجرامي في دولة أخرى.

وتستلزم مثل هذه الجرائم وجود تعاون دولي فعال [1] والذي يعتبر

---

(1) LA COmmision "invite fnstatment les autorites nationals compptentes a cooperer apin de parvenir a un accord international definissant les contenus illegaux et, par consequent, passibles de sanctions quelques soit le lieu de residence du fournisseur de contenu " et " propose Hume'etablissement de catalogues "nationaux " aisement accessibles recensant les contmis ou les operations illegales detectees sur intenrt ",

راجع في ذلك :

La criminamite infromatique sur L'internet

ضروريا من أجل حماية حقيقية لأنظمة الاتصالات البعدية التي تمر بالعديد من الدول وينشأ حتما عن وجود أوجه خلاف بين القوانين الوطنية والخاصة بتقينة نظم المعلومات ما يعرف بالمعلومات المختبئة والذي ستكون لها نتيجة عكسية في صورة قيود وطنية على حرية حركة المعلومات.

وفي مجال الاجراءات فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاما من أجل التيسير دون عقبة لطلب المساعدة القانونية الوطنية ،أنه قد تلتمس إحدى الدول المساعدة القضائية من دولة أخرى بحيث يمكن لهذه الأخيرة أن تباشر التدابير التي تكون طبقا لقوانينها الخاصة .

أولا: التدابير الواجب مباشرتها على المستوى الوطني

يمكن تقسيم هذه التدابير إلى نوعين احداهما تدابير موضوعية والأخرى اجرائية . وسنخصص لكل منهما مطلبا مستقلا وذلك على النحو التالي :

- التدابير الموضوعية [1]:

ينبغي على الدول أن تتبع سياسة جنائية مشتركة تهدف إلى حماية المجتمع من مخاطر الجريمة المعلوماتية وذلك من خلال تبنى التشريعات الملائمة لمواجهة الخطورة المتمثلة في إمكان إستخدام شبكات الكمبيوتر والمعلومات الالكترونية في إرتكاب أفعال إجرامية مع إمكانية تخزين ونقل الدليل المتعلق بمثل هذه الأفعال عبر تلك الشبكات .

لذا من الأهمية بمكان مباشرة التدابير الآتية :

أولا : يجب على كافة الدول أن تتبنى التشريعية وغيرها من التدابير اللازمة لإدراك عملية الدخول غير المشروع إلى سائر أو جزء من أجزاء

(1) راجع في ذلك

European committee on crime problems 9cppc). Committee of experts on crime in cyber – space (pc-cy) draft convention on cybercirm 9draf N19) stansbourg, 25 April 2000

نظام الكمبيوتر كجريمة جنائية وفقا لأحكام قوانينها الوطنية إذا ما ارتكبت هذه الأفعال بصورة عمدية ويجوز لأي دولة أن تحدد من بين متطلبات ارتكاب الجريمة أن يكون ارتكابها من خلال اختراق تدابير الأمن أو بينة الحصول على بيانات الكمبيوتر .

ثانيا : ينبغي على أن تتبنى التدابير التشريعية وغيرها من التدابير اللازمة لإدراك أعمال الاعتراض دون حق والتي تتم بأساليب فنية كعمليات نقل الكمبيوتر إلى أو من خلال حاسب آلي آخر وكذا الاشارات الالكترومغناطيسية الصادرة من أحد نظم المعلومات والتي تحمل مثل تلك البيانات واعتبارها جريمة جنائية لأحكام قوانينها الوطنية إذا ما ارتكبت بصورة عمدية .

ثالثا : يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإدراك أعمال الإضرار أو المحو أو الاتلاف أوالتعديل أو الإعاقة التي تستهدف بيانات الحاسب الآلي بدون وجه حق واعتبارها جريمة إذا ما ارتكبت بصورة عمدية .

رابعا : يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإدراج أعمال الإعاقة الخطرة دون وجه حق بوظائف نظام الكمبيوتر من خلال ادخال أو نقل أو الإضرار أو محو أو اتلاف أو تعديل أو اعاقة بيانات الكمبيوتر وادراكها باعتبارها جريمة جنائية إذا ارتكبت بصفة عمدية .

خامسا : يجب على الدول أن تتبنى التدابير التشريعية اللازمة لامكانية مساءلة الأشخاص المعنوية جنائيا عن الجرائم الناشئة عن نظم المعلومات وذلك في الأحوال التي يؤدي فيها قصور الاشراف أو الرقابة من قبل الشخص الطبيعية إلى تسهيل ارتكابها.

- التدابير الاجرائية [1]:

وتتمثل هذه التدابير على النحو التالي :

أولا : يجب على الدول أن تتخذ التدابير التشريعية التي تخولها سلطة تفتيش :

أ- أحد أنظمة الكمبيوتر أو جزء منه وبيانات الكمبيوتر المختزنة به.

ب- أحد الوسائط التي قد تكون بيانات الكمبيوتر مختزنة به، وذلك في أراضيها أو في أحد الأماكن الأخرى التي تمارس عليها سلطاتها لأغراض التحقيق.

ثانيا : يجب على الدول أو تتخذ التدابير التشريعية اللازمة لتخويل سلطاتها المعنية في اصدار الأمر لأي شخص سواء كان متواجدا في إقليمها في أي مكان آخر عليه سلطاتها السيادية لكي يقدم أي بيانات محددة واقعة تحت سيطرته ومخزنة في أحد أنظمة الكمبيوتر أو أحد الوسائط المستخدمة في تخزين البيانات وذلك بالصورة التي تطلبها تلك السلطات لأغراض التحقيق.

ثالثا : يجب على الدول أن تتبنى التدابير التشريعية اللازمة لتمكين سلطاتها المعنية من الحصول على نسخة حفظ سريعة للبيانات المخزنة في أحد نظم الكمبيوتر وذلك لأغراض التحقيقات وذلك إذا تبين أنها معرضة بصفة خاصة للفقد والتعديل .

رابعا : يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإجبار الشخص الذي تتخذ حياله اجراءات الحفظ المشار إليها سلفا على الاحتفاظ

---

(1) راجع في ذلك

Europan committee on crime problems (cppc) committee of experts on rime in cyber – space (pc – cy0 draft convention on cyber crimd (draft N 10) Strasbourg 25 april 2000

بسرية الاجراءات لمدة محددة من الزمن وفقا للإطار الذي يسمح به القانون الوضعي .

خامسا: يجب على الدول أن تتخذ التدابير التشريعية اللازمة التي تكفل حفظ بيانات النقل والخاصة بأحد الاتصالات المحددة كما تكفل الحفظ السريع لتلك البيانات الخاصة بعملية النقل وبغض النظر إذا كان مقدم الخدمة واحدة أو أكثر ممن شاركوا في عملية نقل هذا الاتصال .

سادسا: يجب على الدول أن تتخذ التدابير التشريعية اللازمة لمد اختصاصها القضائي على أي من الجرائم المشار إليها إذا ما ارتكبت

أ- بصورة كليه أو جزئية على أراضيها أو على متن باخرة أو طائرة أو قمر صناعي يحمل علمها أو مسجل لديها .

ب- من قبل أحد مواطنيها إذا كانت الجريمة من الجرائم المعاقب عليها وفقا لأحكام القانون الجنائي الساري في محل ارتكابه أو إذا كانت الجريمة قد ارتكبت خارج الاختصاص الإقليمي لأي دولة .

- التدابير الواجب مباشرتها على المستوى الدولي [1]:

ويمكن تقسيم هذه التدابير إلى نوعين: **الأولى:** تتعلق بالتسليم **والثاني:** يتعلق بالمعونة المتبادلة .

أ- تسليم المجرم المعلوماتي:

يجب على الدول أن تتعاون بعضها مع البعض ومن خلال تطبيق المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي حيث يجب تسليم

---

(1) راجع في ذلك

Europan committee on crime problems (cppc) committee of experts on rime in cyber – space (pc – cy0 draft convention on cyber crimd (draft N 19) Strasbourg 25 april 2000

مرتكبيها وذلك وفقا لمعيار معين لتكييف الجريمة كجريمة يجوز تسليم مرتكبيها:

أولا : أن يكون الدخول إلى النظام أو البيانات قد تم بدون وجه حق وبنية الاخلال بسرية البيانات أو اعاقة نظام الكمبيوتر .

ثانيا : أن تبرم الدول فيما بينها اتفاقية تسليم مرتكبي الجرائم المعلوماتية .

ثالثا : إذا ما رفض طلب التسليم الصادر في شأن مرتكبي إحدى الجرائم المعلوماتية بناءا على جنسية الشخص المراد تسلميه نظرا لأن طرف المدعى يعتبر أنه يختص قضائيا بالجرمية محل الادعاء، يقوم الطرف المدعي عليه بتقديم القضية إلى سلطاته بغرض السير في الدعوى الجنائية وعلى أن يبلغ الطرف المدعي بالنتائج المترتبة عليه.

ب- المعونة المتبادلة

وتتمثل المعونة المتبادة في الاجراءات التالية :

أولا : يجب على الدول أن تقدم لبعضها البعض المعونة المتبادل وذلك بأكبر قدر ممكن لاغراض التحقيق والاجراءات الخاصة بالجرائم الجنائية المتعلقة بنظم وبيانات الحاسب الآلي .

ثانيا : يجب على الدول أنتقبل وتستجيب إلى طلبات المعونة المتبادلة من خلال وسائل الاتصال السريعة كالفاكس والبريد الالكتروني ،بالقدر الذي يوفر للطرف الطالب المستوى من الأمن والمصادقة.

ثالثا : تخضع المعونة المتبادلة للاشتراطات المنصوص عليها في قوانين الدولة المدعية أو المنصوص عليها بموجب اتفاقيات المعونة المتبادلة.

رابعا : في الأحوال التي يسمح فيها للطرف المدعي عليه بتعليق طلب المعونة المتبادلة على اشتراط وجود جريمة مزدوجة، يعتبر هذا الشرط محل اعتبار وبغض النظر عما إذا كانت قوانين هذه الدولة تضع الجريمة في نطاق ذات تصنيف آخر.

خامسا : تحدد كل دولة سلطة مركزية تنهض بالمسئولين ارسال طلبات المعونة المتبادلة والرد عليها وتنفيذها أو نقلها للسلطات المعنية للتنفيذ.

سادسا : تنفذ طلبات المعونة المتبادلة وفقا للاجراءات التي تحددها الطرف المدعي قما عدا الأحوال التي لا تتصل فيها تلك الاجراءات مع أحكام القانون السائد بالدولة المعدي عليه .

سابعا : يجوز للدولة المدعي عليها أن ترفض طلب المعونة إذا ما توافرت لديها القناعة بأن الالتزام بما ورد بالطلب قد يخل بسيادتها أو أمنها أو نظامها العام أو بأي من مصالحها الأساسية الأخرى.

ثامنا : يجوز للدولة المدعي عليها تأجيل التصرف في الطلب إذا كان هذا التصرف سيخل بالتحقيقات أو اجراءات الادعاء أو الاجراءات الجنائية التي تباشر بمعرفة السلطات المعنية .

تاسعا : يجب على الدول المدعي عليها أن تخطر الدولة المدعية بصورة فورية بنتائج تنفيذ طلب المعونة فإذا ما رفض الطلب أو تم تأجيله يجب تقديم الأسباب إلى الرفض أو التأجيل .

عاشرا: يجوز للدولة المدعية أن تطلب من الدولة المدعي عليها أن تحتفظ بسرية الوقائع والمحتويات التي يتضمنها الطلب ،فإذا لم يكن بمقدور الدولة المدعية عليها الوفاء بمتطلبات سرية الطلب فيجب عليها اخطار الدولة المدعية بذلك وعلى الاخيرة في هذه الحالة تحديد ما إذا كان سينفذ الطلب من عدمه .

الحادي عشر: يجوز في حالة الاستعجال ارسال طلبات المعونة المتبادلة مباشرة إلي السلطات القضائية بما فيها النيابة العامة لدى الدولة الدعية عليها وفي مثل الحالة يجب ارسال نسخة بنفس الطلب إلى السلطة المركزية القائمة لدى الدولة المدعي عليها.

- الإجراءات الوطنية والدولية لمواجهة جرائم الكمبيوتر:

أ-المستوى الوطني :

نظرا لظهور مشكلة جرائم الكمبيوتر كمشكلة أمنية ، وقانونية واجتماعية، فإن خبراء الأمن المعلوماتي وصانعي السياسات الحكومية ومسوقي الكمبيوتر ، والأفراد المهتمين في هذا الموضوع بحاجة إلى تغيير نظرتهم تجاه جرائم الكمبيوتر ، لا لأنها مشكلة وطنية فقط، وإنما كمشكلة عالمية، وتتطلب الإجراءات الوطنية تعاونا في مجال القطاعين العام والخاص،فعلى القطاع الخاص الالتزام بإجراءات الوقاية، وعلى القطاع العام تنفيذ الإجراءات اللازمة لمكافحة الجريمة ،وبوجه عام هناك حاجة إلى تحقيق ما يلي:

1- وجود التشريعات اللازمة لحماية ملكية الكمبيوتر، وللبيانات،والمعلومات والمعدات اللازمة للتشغيل والتوصيل.
2- زيادة الوعي الوطني لجرائم الكمبيوتر وللعقوبات المترتبة عليها.
3- إنشاء وحدات مختصة في التحقيق في جرائم الكمبيوتر في المحاكم والشرطة.
4- إيجاد نوع من التعاون مع الدول الأخرى في الحماية والوقاية من هذه الجرائم.

ب-المستوى العربي:

عقدت الجمعية المصرية للقانون الجنائي مؤتمرها السادس في القاهرة في الفترة من 25 إلى 28 أكتوبر 1993م وناقشت موضوع جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات من خلال الأبحاث والدراسات المقدمة من الباحثين والتي دارت حول تحديد أنواع الجرائم المختلفة المتعلقة بنظم المعلومات من اعتداء مادي على الأجهزة وأدوات

الكمبيوتر بالسرقة أو التخريب أو الإتلاف إلى اعتداء على البيانات والمعلومات المختزنة في قواعد المعلومات بالغش أو التزوير أو السرقة ، والحصول على تلك البيانات والمعلومات دون إذن أو الاتجار فيها، والتحايل على الأجهزة للحصول على الأموال ، وتحويل ونقل الأموال المتحصلة من الجرائم لغسلها.

وأوضحت البحوث والمناقشات أن الاعتداء قد يحث أثناء إدخال البيانات والمعلومات أو إخراجها أو من خلال المعالجة الآلية لها،وذلك بالحذف أو المحو أو الإضافة أو التعديل دون حق،وأن هذه المعلومات قد تكون ثقافية أو سياسية أو عسكرية أو اقتصادية أو علمية أو اجتماعية.

وقد بينت الأبحاث والدراسات والمناقشات صعوبة اكتشاف جرائم نظم المعلومات وإثباتها، وأكدت على ضرورة تدريب رجال الشرطة القضائية ورجال التحقيق ورجال القضاء ، كما حذرت من تزايد احتمالات انتهاك حرمة الحياة الخاصة عن طريق التجسس والتنصت على الكابلات الرابطة بين القواعد الأساسية والوحدات الفرعية.

وفي ختام المؤتمر قد تمكن المؤتمرون من تجريم الأفعال المتعلقة بالكمبيوتر والتوصية باتخاذ التدابير والإجراءات اللازمة والتي تكون على النحو التالي:

- تجريم الأفعال المتعلقة بالكمبيوتر:

1- حصول الشخص لنفسه أو لغيره على أموال عن طريق اختراق نظم المعلومات للاستيلاء علىها دون وجه حق.

2- حصول الشخص لنفسه أو لغيره على بيانات أو معلومات أو مستندات عن طريق اختراق نظم المعلومات دون إذن.

3- حصول الشخص لنفسه أو لغيره على أموال دون وجه حق عن طريق التحايل على الأجهزة.

4- تحويل أموال دون حق عن طريق اختراق الأجهزة.
5- تحويل أموال مستمدة بطريق غير مشروع عن طريق الأجهزة بقصد غسلها وتمويه مصدرها.
6- إتلاف أو تشويه البيانات أو المعلومات أو المستندة المختزنة في قاعدة المعلومات.
7- استخدام المعلومات المختزنة في قاعدة نظم المعلومات بقصد المساس بحرمة الحياة الخاصة للغير أو حقوقهم.
8- تغيير الحقيقة في البيانات أو المعلومات أو المستندات التي تحويها قاعدة نظم المعلومات عن طريق الإضافة أو الحذف أو المحو الكلي أو الجزئي أو التعديل.
9- حصول الشخص على نسخة من البرامج المختزنة في قاعدة نظم المعلومات دون إذن.
10- حصول الشخص على البيانات أو المعلومات أو المستندات التي تحويها قاعدة نظم المعلومات بقصد إفشائها أو قيامه بإفشائها فعلا أو الانتفاع بها بأي طريق.
11- الاطلاع بأي طريق على المعلومات أو البيانات أو المستندات التي تحويها قاعدة نظم المعلومات دون إذن بقصد معرفتها.
12- التسبب خطأ في حصول الغير على أموال أو بيانات أو معدات أو معلومات أو مستندات أو في ارتكاب فعل من الأفعال المذكورة أعلاه.

- الإجراءات والتدابير الواجب إتباعها:

1- مساءلة الأشخاص الطبيعيين والأشخاص المعنويين والمؤسسات الفردية إذا اقترنت الجريمة لصالح الأشخاص والمؤسسات أو بأسمائها بالإضافة إلى مساءلة الأشخاص الطبيعيين من مقترفيها وشركائهم.
2- إدماج نصوص جرائم نظم المعلومات في قانون العقوبات الوطني على أن يفرد لها فصل خاص.

3- تدريب رجال الشرطة القضائية ورجال التحقيق والقضاء على كيفية استخدام أجهزة المعلومات وأدواتها وأشرطتها وآلات الطباعة الخاصة بها والإحاطة بكيفية إساءة استخدامها.

4- تدريب رجال الشرطة القضائية والتحقيق والقضاء على كيفية الكشف عن هذه الجرائم وإثباتها.

5- حث الدول على التعاون فيما بينها خاصة في مجال المساعدات والإنابة القضائية للكشف عن هذه الجرائم، وجمع الأدلة لإثباتها ، وتسليم المجرمين المقترفين لها، وتنفيذ الأحكام الأجنبية الصادرة بالإدانة والعقوبة على رعايا الدولة المقترفين لها بالخارج.

ومن جانب آخر تعكف جامعة الدول العربية ممثلة في الأمانة العامة لمجلس وزراء الداخلية العرب على إعداد مشروع اتفاقية عربية لجرائم الكمبيوتر وكذلك إنشاء لجنة تتألف من ممثلي عدد من الدول الأعضاء لمتابعة كافة المستجدات التقنية والاتفاقيات الدولية المتعلقة بجرائم الكمبيوتر والعمل على توحيد التشريعات العربية بهذا الشأن.

ج-المستوى الدولي :

الجرائم المتعلقة بالكمبيوتر تتضمن موقفا متحولا أو متنقلا، أو متحركا وذلك بسبب طبيعة الكمبيوتر .فان إمكانية التخزين متزايدة وكذلك التحريك، وانتقاء البيانات من خلال الاتصال من مسافة بعيدة،والقدرة على الاتصال ونقل البيانات وتحويلها بين الكمبيوتر من مسافات كبيرة.وكنتيجة لذلك فان عدد الأمكنة والدول التي يمكن أن تكون متورطة في حالات جرائم الكمبيوتر في تزايد.وقد ترتكب الجريمة في نظام عدلي معين وجزئيا في نظام ثان وثالث ومن أي مكان في العالم.

ومع خاصة الحد المتحرك فانه لا بد من تحديد مكان وقوع الجريمة حيث أن أي نظام قضائي يجب أن يتعامل معها(التحقيق والمحاكمة). أما إذا

كانت الجريمة تتطلب تدخل دولتين فان تصارع الأنظمة القضائية أمر وارد، إذا لم يكن هناك اتفاقيات ثنائية أو قانون دولي تلتزم بع الأطراف المعنية.

ويرتبط مع مشكلة الحد المتحرك، مشكلة تتعلق بسيادة الدولة في سن التشريعات للأفعال التي تحصل على أراضيها،والسؤال هنا كيف يتحدد مكان الجريمة،فبعض الدول ترى أن مكان ارتكاب الجريمة يمكن تحديده على مبدأ الوجود في الوقت ذاته حيث يمكن تحديد مكان جريمة بناء على حدوثها في مكان ما أو جزء منها.

أما المبدأ الثاني في تحديد الجريمة فيعتمد على مكان الأثر ،فالمكان الذي يظهر فيه أثر الجريمة يعد مكان ارتكابها، وهذا المبدأ مقبول في دول كثيرة، خاصة الأوروبية. وهنا تصبح جرائم الكمبيوتر ذات صلة.(فالفرد الذي يضغط على لوحة مفاتيح الكمبيوتر في بلد (أ)يمكن أن يدخل على بيانات في بلد (ب) ويمكن أن يحولها إلى بلد (ج)، مثل تحويل العملات أو الحوالات المالية.

وتظهر مشكلة أخرى وهي تتعلق بالسلوكيات المنحرفة في الجرائم ذات الصلة بالكمبيوتر وهي تتعلق باستخدام فيروسات الكمبيوتر، فإذا تمكن شخص ما من دخول قاعدة البيانات لأحد البنوك، وغذاها بأحد الفيروسات، وكان هذا الفيروس مبرمجا بحيث ينقل نفسه إلى بلاد أخرى، أو مدن أخرى.

وعندما يدمر الفيروس برنامج أحد البنوك، فان الأثر الناجم عن ذلك يظهر في أكثر من دولة، فأي من هذه الدول لها حق التحقيق والحكم في هذه الجريمة. إن مكان الجريمة هو مكان استخدام الكمبيوتر في تنفيذ العملية(بلد - أ) أم البلد الذي تحولت إليه البيانات(بلد - ب)، والمبدأ الأكثر تطبيقا فيما يتعلق بالجرائم المتصلة بالكمبيوتر يقود إلى نتيجة مفادها أن مكان جريمة الكمبيوتر يتحدد في المكان الذي حصل فيه أحد أجزاء هذه الجريمة، وهذا يتطلب تنسيقا دوليا بين أنظمة العدالة المختلفة فيما يتعلق بالمحاكمة، والعقوبة....

والأساس الآخر يكمن في تطبيق القانون في حالات العناصر الموجودة خارج حدود الدولة، فيما يتعلق بالاحتيال، والتخريب، والاستخدام غير المشروع... بواسطة الكمبيوتر أو للمعلومات الموجودة فيه. والموضوع المشار إليه هنا هو الحماية لبعض أنواع التعديات والجرائم المتصلة بالكمبيوتر في مواضيع الاقتصاد، أو البيانات الحكومية... الحكومات توسع نطاق نظامها العدلي إلى خارج حدودها لحماية أمنها الداخلي.

أما مشكلة الدخول المباشر حيث أن التقنيات الحديثة جعلت من الممكن أن تكون البيانات متوافرة في بلد ما بينما هي مخزنة في بلد آخر، وهذا الموقف أصبح منتشرا خاصة في شبكات المعلومات الدولية.وهناك من ينظر أن الدخول لقواعد المعلومات الوطنية من خارج الحدود الجغرافية يعد تدخلا في استقلالية الدولة وسيادتها .

وبما أن العالم مترابط إلكترونيا، فيجب الاهتمام على المستوى الدولي بمشكلة جرائم الكمبيوتر وخاصة في مجال التشريعات والتعاون المتبادل، ويعتقد مركز الأمم المتحدة للتطوير الاجتماعي والشؤون الإنسانية أن الوقاية من جرائم الكمبيوتر تعتمد على الأمن في إجراءات معالجة المعلومات، والبيانات الإلكترونية، وتعاون ضحايا جرائم الكمبيوتر،ومنفذي القانون،والتدريب القانوني، وتطور أخلاقيات استخدام الكمبيوتر.والأمن الدولي لأنظمة المعلومات. ففي المجال الدولي هناك حاجة للتعاون المتبادل بين الدول، والبحث الجنائي والقانوني فيما يتعلق بهذا العالم الجديد الذى يحتاج منا المزيد من الجهد لسبر أغواره والتعمق فيه أموره، فعلى سبيل المثال، قدمت لجنة جرائم الكمبيوتر بالاتحاد الأوروبى توصيات تتعلق بجرائم الكمبيوتر تمحورت في النقاط التالية:

1- المشكلات القانونية في استخدام بيانات الكمبيوتر والمعلومات المخزنة فيه في التحقيق الجنائي.

2- الطبيعة العالمية لبعض جرائم الكمبيوتر.
3- تحديد معايير لوسائل الأمن المعلوماتي وللوقاية من جرائم الكمبيوتر.
4- مشكلة الخصوصية وخرقها في جرائم الكمبيوتر.
5- موقف ضحايا جرائم الكمبيوتر.
6- إدراك أهمية الاستجابة الدقيقة والسريعة للتحدي الجديد للجرائم المتصلة بالكمبيوتر.
7- أن يؤخذ بالحسبان أن الجرائم المتصلة بالكمبيوتر ذات خاصية تحويلية.
8- الوعي بالحاجة الناجمة للتناغم بين القانون والتطبيق وتحسين التعاون الدولي القانوني.



خاتمـــة

تناولنا فى هذا الكتاب، الجرائم الإلكترونية فى مصر والعالم العربى فى أسلوب مقارن مع الدول الأوروبية والولايات المتحدة الأمريكية، وقد ركزنا على تبيان الفرق بين الجرائم الواقعة على جهاز الحاسب ذاته والجرائم الإلكترونية الأخرى والتى منها جرائم المعلوماتية والإنترنت. وقد انتشرت جرائم المعلوماتية والانترنت بشكل كبير، وترتب على هذا الانتشار أضرارا بالغة فى حق الأفراد والمؤسسات بل والدول ذاتها، فمنظومة الأمن القومى لأى من الدول قد يخترقها أى من المجرمين الإلكترونيين كالهاكرز مثلا، فالأمر لا يحتاج أكثر من شخص اعتاد الإجرام الإلكترونى لكى يقوم باختراق مواقع الجهات السيادية والاطلاع على أسرارها وخصوصياتها. فضلا عن ذلك فالجرائم الإلكترونية، تأتى على أشكال وتصنيفات متنوعة، كما أن المجرم الإلكترونى له صفات خاصة تختلف عن تلك التى يتصف بها المجرم العادى.

ولاشك أن الجريمة الإلكترونية، ليست حكرا على بعض الدول دون الآخر، إذ أن الواقع الذى يفرضه التقدم التكنولوجى والمعلوماتى والذى أكده التطور المستمر فى وسائل معالجة ونقل المعلومات باعتبارها باتت المحدد الاستراتيجي للبناء الثقافي والإنجاز الاقتصادي، يؤكد أن هذه الجريمة الجديدة، آخذة فى الانتشار فى ربوع الأرض، فليس غريبا أن نجد مجرمى المعلوماتية والإنترنت فى العالم العربى وفى مقدمتهم مصر، كما أن الدول الأوربية والولايات المتحدة الأمريكية ظلت لفترة طويلة – وما زالت- مرتعا خصبا للإجرام الإلكترونى بل إن هذه الدول بما حققته من تقدم علمى وتكنولوجى كانت أحد الأسباب الرئيسية لانتشار الجريمة الإلكترونية فى ربوع العالم.

وأمام هذا الانتشار الكبير لهذا النوع من الجرائم اتجهت الدول إلى تضمين أنظمتها القانونية قوانين لمكافحة الجريمة الإلكترونية من أجل إنزال حكم القانون على المجرم المعلوماتى أينما وجد وتوقيع العقاب عليه. فضلا عن اتجاه الكثير من الدول إلى تفعيل مبدأ التعاون الدولى فى مجال مكافحة الجريمة الإلكترونية.

ومما هو جدير بالذكر أن الجرائم الإلكترونية، هى ظاهرة إجرامية جديدة ومستجدة تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن جريمة الحاسب الآلي التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، فجريمة الحاسب الآلي جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات.

هذه المعطيات هي موضوع هذه الجريمة وما تستهدفه اعتداءات الجناة، وهذا وحده - عبر دلالته العامة - يظهر مدى خطورة الجرائم الإلكترونية، فهي تطال الحق في المعلومات، وتمس الحياة الخاصة للأفراد، وتهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري، لذا فإن إدراك ماهية الجرائم الإلكترونية ، منوط بتحليل وجهة نظر الدارسين لتعريفها والاصطلاحات الدالة عليها واختيار أكثرها اتفاقا مع الطبيعة الموضوعية لهذه الجرائم، واستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها وسمات مرتكبيها ودوافعهم.

وحرى بنا التأكيد على ما أثاره إحصاء إجراءات تقنية المعلومات من تحديات لها وزنها بالنسبة لقانون العقوبات في كل الأنظمة القانونية ويرجع

السبب في ذلك إلى حقيقة مؤداها أنه حتى هذه اللحظة، فإن الأشياء المادية والمرئية هي التي تكون محمية بالقوانين الجنائية، وحماية المعلومات والقيم المعنوية الأخرى - وإن وجدت منذ فترة زمنية قصيرة- إلا أنها حتى منتصف القرن العشرين كانت أقل أهمية، وقد طرأ تغيير جوهري على هذا الموقف أثناء العشر سنوات الأخيرة، حيث أدى تطور المجتمع من مجتمع صناعي إلى مجتمع ما بعد الصناعي، إلى تزايد قيمة المعلومات بالنسبة للاقتصاد والمجتمع والسياسة، فضلا عن الأهمية المتنامية لتقنية المعلومات خلال فترة زمنية قصيرة، وهو الأمر الذى أوجد ما أصبح يعرف بقانون المعلومات.

ووفق ضوء ما تقدم يمكننا القول بأن هذا الكتاب يتناول موضوع الثورة المعلوماتية من زاوية الجانب السلبى منها والمتعلق بجرائم المعلوماتية وتأثيره على مكونات المجتمع. وأمام هذا الشكل الجديد من الإجرام لا تبدو قوانين العقوبات الوطنية في حالتها الراهنة كافية أو فعالة على النحو المطلوب أو المرضي فنصوصها والنظريات والمبادئ القانونية التي تتضمنها أو تقف ورائها موروث بعضها من القرن 19 حيث لم يكن هناك فنيين حينذاك وإنما أصحاب مهن وحرفيين.

وتطبيق بعض قواعد قوانين العقوبات الحالية على أشكال جديدة من الجرائم كتلك التى ترتب على استخدام تقنيات الحاسبات الآلية والمعلومات وأساليبها، ستواجه بصعوبات جمة منها صعوبات ناجمة عن الطبيعة الخاصة والخصائص الفنية الفريدة للوسائل المعلوماتية المستخدمة في ارتكابها، فضلا عن الصعوبات الرئيسية الأخرى والمتعلقة بنصوص التجريم التقليدية التى وضعت في ظل تفكير يقتصر إدراكه على الثروة الملموسة والمستندات ذات

الطبيعة المادية مما يتعذر معه تطبيقها لحماية القيم غير المادية المتولدة عن المعلوماتية.

إن وسائل الاتصال لم تخترع الجريمة، بل كانت ضحية لها في معظم الأحوال حيث أن هذه الوسائل تعرضت لسوء الاستغلال من قبل كثيرين ، ومن الثابت أيضا أن المجرمين وظفوا الاتصال تاريخيا لخدمة النشاطات الإجرامية التي يقومون بها. أما الجريمة فهي ذاتها الجريمة في قديم التاريخ، وحديثه، لا يختلف على بشاعتها، وخطرها على المجتمع الإنساني أحد، ولذلك اتفق على مواجهتها، ومن أجلها أقيمت المحاكم، وسنت العقوبات.

ومما لا شك فيه أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الأفعال الإجرامية التقليدية، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع في ارتكاب الفعل غير المشروع، فضلا عن ذلك، تتمتع جرائم الكمبيوتر والمعلوماتية بعدد من الخصائص التى تختلف تماما عن الخصائص التى تتمتع بها الجرائم التقليدية، كما أن الجانى الالكترونى(أو المجرم الالكترونى) يختلف أيضا عن المجرم العادى.

ويأتي في مقدمة أسباب الجريمة المعلوماتية، غاية التعلم والتي تتمثل في استخدام الكمبيوتر والإمكانيات المستحدثة لنظم المعلومات وهناك أمل الربح وروح الكسب التي كثيرا ما تدفع إلى التعدي على نظم المعلومات بالإضافة إلى الدوافع الشخصية والمؤثرات الخارجية التي قد تكون سببا في ارتكاب الجريمة المعلوماتية.

وعلي الرغم من انتشار جرائم المعلوماتية في مصر فى ظل جهود الحكومة المصرية من أجل جذب الاستثمارات في مجال التكنولوجيا إلا ان هناك فراغا تشريعيا في هذا المجال خاصة في قضايا النشر الالكتروني وقوانين جرائم الانترنت الخاصة باقتحام النظم وغيرها، فلا يوجد فى مصر نظام قانوني

خاص بجرائم المعلومات، إلا أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية.

وقد أرجع المتخصصون هذا الفراغ من أية عقوبات خاصة بجرائم الانترنت فى التشريع المصرى إلى حداثة هذا المجال الذي لم يتعد عمره سنوات قليلة وما يطبق حاليا علي جرائم الانترنت هو القانون التقليدى الذى يتم بموجبه على الجرائم العادية مثل جريمة سرقة، حيث يعاقب مرتكبها بالحبس مدة لاتقل عن 24 ساعة ولاتزيد علي ثلاث سنوات وجريمة النصب التى يعاقب مرتكبها بعقوبة النصب المدرجة في قانون العقوبات.

أما السب والقذف الالكترونى، فتكون جنحة، وإذا كانت الجريمة تركيب صور فاضحة، توجه لمرتكبها، تهم خدش الحياء وهتك العرض والتحريض علي الفسق. أما اطلاق الشائعات والسطو علي أرقام الكروت الائتمانية واقتحام نظم البنوك فتوجه إلي مرتكبها تهم تكدير الأمن العام وتهديد الاقتصاد القومي والاضرار بالمصالح العليا للبلاد وهي اتهامات خطيرة تقود صاحبها الي محاكم الجنايات مباشرة. على أن هذا التكييف القانونى لجرائم المعلوماتية يظل عاجزا عن مواكبة هذه النوعية من الجرائم وما يصاحبها من تطور مستمر فضلا عن تنامى أنواعها وانتشارها بشكل مريب وهو الأمر الذى يحتم على المشرع المصرى سرعة اصدار قانون جديد يواجه الجرائم الالكترونية خاصة ان هناك بعض الجرائم المستحدثة التي لن تجد لها تكييفا قانونيا محددا في القانون التقليدى.

وفيما يتعلق بآليات مواجهة الجرائم المعلوماتية، فلا أحد ينكر الجهود الحكومية والأهلية فى مجال المكافحة، فقد أنشأت وزارة الداخلية المصرية عام 2002، آلية فى هذا الاطار تحت مسمى " إدارة مكافحة جرائم الحاسب

الآلي وشبكة المعلومات التابعة للادارة العامة للمعلومات والتوثيق، بالقرار الوزارى رقم 13507 لسنة 2002، هذا فضلا عن الجمعية المصرية لمكافحة جرائم المعلوماتية والإنترنت ودورها فى هذا المجال.

ويؤكد الكثير من رجال القانون على ضرورة إنشاء محكمة إلكترونية لسد الفجوة القانونية التي أحدثها التطور التكنولوجي الهائل في السنوات الأخيرة، فهناك جرائم ترتكب، وحرمات تنتهك، وحقوق تسلب على شبكة الإنترنت دون رقابة قانونية تذكر، والسبب في ذلك عدم وجود قانون دولي رادع يلاحق هواة الإجرام الإلكتروني، ويحاكمهم أمام محاكم دولية، إلا أن ذلك ليس من الأمور البعيدة التي يمكن أن تشق طريقها إلى التطبيق العملي في المستقبل القريب.

والمحكمة الالكترونية تتطلب إصدار تشريعات متخصصة فى مجال مكافحة الجريمة الإلكترونية، فضلا عن توفير القضاة المتميزين للقيام على أعمال الفصل فى القضايا المطروحة على هذه المحاكم.

وغنى عن البيان أن الدول العربية ليست ببعيدة عن مرمى الجرائم الإلكترونية، ذلك أن هذه الجرائم لم تترك بلدا من بلاد العالم إلا واخترقتها ونالت من أهداف محدده فيها، فالسعودية والإمارات وسلطنة عمان والكويت فلسطين وغيرهم من الدول العربية بادروا إلى وضع - أو فى طريقهم لوضع- تشريعات إلكترونية لمواجهة الجرائم المعلوماتية.

وبالنظر إلي موقع العالم العربي في خريطة استخدام وسائل تقنية المعلومات الحديثة وموقع الدولة بين شقيقاتها الدول العربية فإن إحصائيات الاتحاد الدولي للاتصالات لعام 2001 تشير إلى أن نسبة مواطني العالم العربي، الذين سبق أن استخدموا شبكة الإنترنت، لا يتعدى 1% رغم أن سكان العالم العربي ال 170 مليون نسمة يشكلون5%من مجموع سكان العالم.

وإذا ما قارنا ذلك بنسبة الأوروبيين والأمريكيين التي تفوق 58 في المائة فإن ذلك يدفع البعض إلى وصف تجربة العالم العربي في مجال تكنولوجيا الاتصالات والإنترنت بأنها في مرحلتها "الجنينية".

وإذا لم يكن الحاجز أخلاقيا أو سياسيا فقد يكون تقنيا أو ماليا. إذ تعد معظم شبكات الاتصال في العالم العربي غير متطورة وملكا للقطاع العام. كما تتباين نسبة توفير خدمات الاتصال من بلد عربي لآخر، ففي الوقت الذي نجد فيه أكثر من 100 خط هاتفي لكل 100 منزل في الإمارات والكويت، لا تتعدى النسبة في سوريا ومصر والمغرب حيث الكثافة السكانية كبيرة، خمسين خط هاتفي لكل مائة عائلة.

على أن ذلك لا يمنع من وقوع خسائر هائلة فى الدول الأوروبية من جراء الجرائم المعلوماتية، وهو الأمر الذى دفع هذه الدول إلى الإهتمام بسن قوانين وطنية لمكافحة هذه الجرائم السعى لتطبيقها أمام القضاء الوطنى فيها مع وضع الآليات اللازمة لمكافحة الجريمة الإلكترونية فى الدول الغربية.

هذا ويلزم للمجتمع المعلوماتى فى مجال قانون الاجراءات الجنائية أن ينشئ قواعد قانونية حديثة بحيث تضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق فى مجال جرائم الكمبيوتر.

والسبب فى ذلك أن محترفى انتهاك شبكات الحاسبات الآلية ومرتكبى الجرائم الاقتصادية وتجار الأسلحة والمواد المخدرة يقومون بتخزين معلوماتهم فى أنظمة تقنية المعلومات وعلى نحو متطور. وتصطدم الأجهزة المكلفة بالتحقيق بهذا التكنيك لتخزين المعلومات وهى التى تسعى للحصول على أدلة الاثبات.

ونظرا لسهولة حركة المعلومات فى مجال أنظمة تقنية المعلومات حيث تجعل هذه السهولة لحركة المعلومات أنه بالإمكان ارتكاب جريمة عن طريق حاسب آلي موجود فى دولة معينة بينما يتحقق نتيجة هذا الفعل الاجرامى فى

دولة أخرى، وهو الأمر الذى استلزم ضرورة وجود تعاون دولى محكم فى مجال مكافحة هذا النوع من الجرائم ولأجل توفير حماية حقيقية لأنظمة الاتصالات.

ونظرا للخطورة التى تمثلها الجرائم الإلكترونية فقد تناولت التشريعات المقارنة أنواعها بشيء من العناية والاهتمام، حيث ركزنا على جريمة العدوان على الإئتمان الرقمى و جريمة الاحتكار والاحتكار المضاد وجرائم الأخلاق، وجريمة الترويج السمعى-المرئى الفاضح، وجريمة البث العلنى وتشمل النشر والسب والقذف والتشهير والمراسلة وجريمة المطاردة والإزعاج وجريمة العدوان على التشفير باعتبار أن هذه جميعا تدخل فى عداد الجرائم الإلكترونية التى تستحق المواجهة التشريعية والتعاون الدولى لمواجهتها.

وعلى أية حال فإنه فى سبيل الحد من الجرائم الإلكتورنية، فيجب ان نضع فى الاعتبار المقترحات والحلول اللآتية:-

1- ضرورة تقنين قواعد جديدة لمكافحة الجرائم المعلوماتية ؛ تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم
ولاسيما فيما يتعلق بالإثبات في الدعاوى الناشئة عن هذه الجرائم ؛ سواء في ذلك الدعاوى لجنائية والمدنية والتأديبية. كما ينبغي تعديل قواعد الإجراءات الجنائية لتتلاءم مع هذه الجرائم.

2- ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم المعلوماتية .

3- ضرورة تخصيص شرطة خاصة لمكافحة الجرائم المعلوماتية ؛ وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت.

4- يتعين تدريب وتحديث رجال الادعاء العام – أو النيابة لعامة – والقضاء بشأن التعامل مع أجهزة الحاسوب والإنترنت .

5- ينبغي أن تنص التشريعات العربية-مثلا- على اعتبار أن الانترنت يعتبر وسيلة من وسائل العلانية في قانون العقوبات والقوانين ذات الصلة بالجرائم المعلوماتية ؛ مع الأخذ بعين الاعتبار أن الإنترنت أوسع انتشارا من سائر وسائل النشر والعلانية الأخرى .

6- يلزم تعديل قوانين ونظم الإجراءات الجزائية (الجنائية) ؛ بالقدر الذي يسمح ببيان الأحكام اللازم إتباعها حال التفتيش على الحاسبات وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني حتى يستمد الدليل مشروعيته .

7- ينبغي أن يسمح للسلطات القائمة بالضبط والتحقيق بضبط البريد الإلكتروني وأية تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل ؛ والكشف عن الحقيقة .

8- يلزم أن تمتد إجراءات التفتيش إلى أية نظم حاسب آلي أخرى ؛ يمكن ان تكون ذات صلة بالنظام محل التفتيش وضبط ما بها من معلومات.

ويشترط في هذه الحالة أن يكون هذا الإجراء ضروريا، والقاعدة العمة – في هذا الشأن – الضرورة تقد بقدرها.

9- يتعين أن تكون للسلطات لقائمة بالضبط والتفتيش : سلطة توجبه أوامر لمن تكون لديه معلومات خاصة للدخول على ما يحويه الحاسب الآلي والانترنت من معلومات للإطلاع عليها .

10- ضرورة النص صراحة في القوانين المنظمة للإثبات – الجنائي والمدني – بما يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والانترنت في الإثبات ؛ طالما أن ضبط هذه الأدلة جاء

وليدة إجراءات مشروعة، على أن تتم مناقشة هذه الأدلة بالمحكمة وبحضور الخبير؛ وبما يحقق مبدأ المواجهة بين الخصوم .

11- يتعين اعتبار نشر وطباعة الصور الجنسية عن طريق الانترنت مما يدخل ضمن زمرة جرائم الآداب .

12- ضرورة تجريم استخدام الأطفال في تصوير أفلام تمثلهم في أوضاع مخلة بالآداب العامة وعرضها على شبكة الانترنت وباستخدام البريد الإلكتروني.

13- يتعين النص صراحة على تجريم الدخول غير المصرح به على البريد الإلكتروني لإتلاف محتوياته أو إرسال صور إباحية أو تغيير محتواه أو إعاقة الرسائل أو تحويرها عبر الانترنت .

14- ضرورة سن التشريعات لمكافحة جرائم الإنترنت، وذلك بإدخال كافة صورالسلوك الضار والخطر على المجتمع التي يستخدم فيها انترنت .

15- يتعين اتاحة الفرصة للمواطنين في المشاركة في مكافحة الجرائم المعلوماتية ؛ وذلك من خلال إيجاد خط الساخن يختص بتلقي البلاغات المتعلقة بهذه الجرائم؛ ولاسيم الجرائم الأخلاقية كحالات الإعلان عن البغاء وممارسة الفجور أو الاستغلال الجنسي للأطفال عبر الانترنت .

16- ضرورة نشر الوعي بين صفوف المواطنين – ولاسيما الشباب – بمخاطر التعامل مع المواقع السيئة علي شبكة الإنترنت ؛مع ضرورة نشر الوعي المجتمعي بالمخاطر النفسية والاجتماعية وغيرها الناجمة عن الاستخدامات غير الآمنة للانترنت وتكثيف التوعية عن الآثار السلبية الصحية المترتبة عن الممارسات الجنسية الشاذة ومعاشرة البغايا؛ وذلك بأسلوب غير مباشر من خلال المواد الدرامية .

17- يتعين إدخال مادة "أخلاقيات استخدام الانترنت" ضمن المناهج الدراسية في التعليم ماقبل الجامعي .

18- إنشاء قسم جديد بكليات الحقوق بالجامعات العربية لدراسة الحماية القانونية للمعلوماتية أو تحت مسمى آخر "قانون المعلوماتية والانترنت" أو "قانون الحاسب الآلي والانترنت".

19- تفعيل دور المجتمع المدني ولاسيما الجمعيات الأهلية للقيام بدورها في وقاية الشباب من الوقوع في الممارسات الخاطئة للسلوكيات والممارسات الضارة أخلاقيا عبر شبكة الانترنت .

20- من المناسب تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية ؛ وخصوصا الإنتربول.

وفي هذ المقام من الممكن أن تنضم الدول العربية إلى الاتفاقات الدولية الخاصة بمكافحة جرائم الانترنت وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية والانترنت والعمل على دراسة ومتابعة المستجدات على الساحة العالمية.

21- أن تسعي الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم المعلوماتية عبر الانترنت؛ مع تشجيع قيام إتحادات عربية تهتم بالتصدي لجرائم الانترنت وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي، ويكون من الأفضل إنشاء شرطة عربية تهتم بمكافحة الجرائم المعلوماتية.

22- نأمل أن يتم التنسيق بين دول مجلس التعاون الخليجي بشأن مكافحة الجرائم المعلوماتية.

توصيات:

كما أن هناك عدد من التوصيات المهمة التى يجب أن تؤخذ بعين الاعتبار ومنها:

1- الإسراع في إقرار وإصدار مشروعات القوانين المتعلقة بجرائم الكمبيوتر والإنترنت والمعلوماتية.

2- عدم إجراء القياس في مجال الجرائم والعقوبات.

3- تشكيل لجنة استشارية علمية تقوم بإعداد الأبحاث والدراسات والاطلاع على التشريعات المتعلقة بمثل هذه المواضيع وتزويد الجهات المعنية بها.

4- تشكيل طاقم فني قانوني يكون على قدر كبير من الدراية والخبرة في مجال الكمبيوتر والإنترنت والمعلوماتية لصياغة قواعد وأحكام مشاريع القوانين المتعلقة بهذا الموضوع.

5- العمل إلي أقصى -حد ممكن- على الاستفادة من الخبراء المتخصصين في مجال الكمبيوتر والإنترنت وكذلك أساتذة القانون الجنائي غير التقليديين.

6- إن إيجاد تشريع عربي نموذجي موحد بشأن جرائم الكمبيوتر يعتبر خطوة في الاتجاه الصحيح تساعد كافة الدول العربية في تطوير تشريعاتها الخاصة بهذه الجرائم واللحاق بالتطورات التي وصلت إليها المجتمعات الصناعية المتطورة.

7- الاستفادة من التجربة الأوروبية قدر الإمكان في مجال معالجة جرائم الكمبيوتر لا سيما الاتفاقية الأوروبية فى مجال مكافحة الجريمة الإلكترونية.

المراجــع

أولا: باللغة العربية:

أ-المراجع العامة:

الأستاذ/ أحمد أمين:

- شرح قانون العقوبات الأصلى – القسم الخاص1923.

د. أحمد فتحى سرور:

- الوسيط فى قانون العقوبات، القسم الخاص-1979.

د. أحمد محمد محرز:

- القانون التجارى،1987/1986.

د. أكثم أمين الخولى:

- الأموال التجارية، مطبعة نهضة مصر بالفجالة – القاهرة 1964.
- الوسيط فى الأعمال التجارية – القاهرة 1964.

د.حسام الدين كامل الأهوائى:

- أصول القانون، بدون ناشر،1988.

د.حسن صادق المرصفاوى:

- جرائم المال، سنة 1956.

د. سميحة القليوبى:

- القانون التجارى، دار النهضة العربية، طبعة عام1976/75.
- الوجيز فى التشريعات الصناعية، القاهرة،1967.

د.رؤوف عبيد:

- جرائم الاعتداء على الأشخاص، دار الفكر العربى،1985.
- جرائم الاعتداء على الأشخاص والأموال، الطبعة السابعة، 1978.

د. عبد الحميد الجمال:

- مبادئ القانون الكتاب الثانى، العلاقات القانونية، الفتح للطباعة والنشر، الإسكندرية، 1990.

د. عبد الرزاق السنهورى:

- الوسيط فى شرح القانون المدنى، القاهرة 1968.

د. عبد العظيم مرسى وزير:

- شرح قانون العقوبات- القسم الخاص- جرائم الاعتداء على الأموال، دار النهضة العربية 1993.

د.عبد الفتاح الصيفى:

- قانون العقوبات اللبنانى – جرائم الاعتداء على أمن الدولة وعلى الأموال، دار النهضة العربية، بيروت 1972.

د. عبد المهيمن بكر:

-القسم الخاص فى قانون العقوبات، الطبعة السابعة 1977.

د. عمر السعيد رمضان:

– شرح قانون العقوبات، القسم الخاص، دار النهضة العربية 1975.

د. عوض محمد:

-جرائم الأشخاص والأموال، دار المطبوعات الجامعية، الإسكندرية.

- قانون الإجراءات الجنائية، الجزء الأول،1989، مؤسسة الثقافة

د. فوزية عبد الستار:

- شرح قانون العقوبات، القسم الخاص، دار النهضة العربية،1983.

د. محسن شفيق:

- القانون التجارى، القاهرة،1949.

د . محمد زكى:

- الإثبات فى المواد الجنائية، بدون ناشر،ص16.

د. محمد محيى الدين عوض:

- القانون الجنائى، جرائمه الخاصة 1979/1978.
- قانون العقوبات السودانى.

د. محمد مختار بربرى:

- قانون المعاملات التجارية، دار الفكر العربى، سنة 1987.

د.محمود محمود مصطفى:

- القسم الخاص، دار النهضة العربية، الطبعة الثامنة 1984.

د. محمود مصطفى القللى:

- شرح قانون العقوبات فى جرائم الأموال، الطبعة الأولى،1939.

د. محمود نجيب حسنى:

- جرائم الاعتداء على الأموال فى قانون العقوبات اللبنانى، دار النهضة العربية، بيروت 1969.
- شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، 1988.
- دروس فى قانون العقوبات، القسم الخاص، دار النهضة العربية 1970.

مصطفى الجمال:

- مبادئ القانون، الكتاب الثانى، العلاقات القانونية، الفتح للطباعة والنشر، الإسكندرية، 1990.

د. نبيل إبراهيم سعد:

- المدخل إلى القانون الكتاب الثانى، نظرية الحق، دار النهضة العربية، بيروت 1995.

د. يسر أنور ود.آمال عثمان:

- شرح قانون العقوبات، القسم الخاص، الجزء الأول1975.

ب- المراجع المتخصصة:

د. أبو اليزيد على المتيت:

- الحقوق على المصنفات الأدبية والفنية والعلمية، منشأة دار المعارف، الإسكندرية، الطبعة الأولى 1967.

آمنة على يوسف:

- قراصنة أنظمة الكمبيوتر، المؤتمر القومى الثالث عشر لأمن الكمبيوتر، ديسمبر 1998.

انتصار .نورى الغريب..

– أمن الكمبيوتر والقانون. دار الراتب العالمية ، لبنان،1994.

د. جلال أحمد خليل

- النظام القانونى لحماية الاختراعات ونقل التكنولوجيا إلى الدول النامية، جامعة الكويت،1992.

د. جميل عبد الباقى الصغير:

- القانون الجنائى والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناتجة عن استخدام الحاسب الآلى ، الطبعة الأولى، دار النهضة العربية، 1992.

- الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية. 1990.

د. طارق سرور:

- كلية الحقوق جامعة القاهرة،ذاتية جرائم الإعلام الإلكتروني (دراسة مقارنة) الطبعة الأولى – دار النهضة النهضة العربية .2001

د. عمر الفاروق الحسينى:

- المشكلات العامة فى جرائم الحاسب الآلى وأبعادها الدولية، دراسة تحليلية نقدية بنصوص التشريع المصري مقارنا بالتشريع الفرنسى ، الطبعة الثانية،1994.

د. غانم محمد غانم:

- عدم ملائمة القواعد التقليدية فى قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت- الإمارات، مايو 2000.

د. ماجد عمار:

- المسئولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، 1989، ص35.

د. محمد حسام لطفى:

- الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر. القاهرة 1987.

د. محمد حسنى عباس:

- الملكية الصناعية والمحل التجاري، القاهرة،1977.

د.محمد سامى الشوا:

- ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، الطبعة الثانية 1998.

د. محمد محي الدين عوض:

- مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات – القاهرة 1993.

د.هاني دويدار:
- نطاق احتكار المعرفة التكنولوجية بواسطة السرية، دار الجامعة الجديدة،1996.
د. هدى حامد قشقوش:
- جرائم الحاسب الالكتروني فى التشريع المقارن، دار النهضة العربية 1992.
د. هشام محمد فريد رستم:
- قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة أسيوط 1994.
د. هلالي عبد اللاه أحمد:
- تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، طبعة،1997 دار النهضة العربية.

جـ- الرسائل:

د. خالد حمدي عبد الرحمن:
- الحماية القانونية للكيانات المنطقية، رسالة دكتوراة، حقوق عين شمس 1992.
د. عبد القدوس عبد الرازق محمد:
- التأمين من المسئولية وتطبيقاته الإجبارية المعاصرة ، دراسة مقارنة بين قانون المعاملات المدنية لدولة الأمارات العربية المتحدة وبين القانون المصرى" رسالة دكتوراة، جامعة القاهرة ، سنة 1999.
د. عزة محمود أحمد خليل:
- مشكلات المسئولية المدنية فى مواجهة فيروس الحاسب. رسالة دكتوراة مقدمة إلى حقوق القاهرة ،عام 1994.

د. عمرو ابراهيم الوقاد:

- النظرية العامة للإختلاس فى جرائم المال الخاص. رسالة دكتوراة، حقوق عين شمس.

د. محمد محمد عنب:

- معاينة مسرح الجريمة، رسالة دكتوراة، أكاديمية الشرطة، كلية الدراسات العليا القاهرة 1988.

د. يونس خالد عرب مصطفى:

- جرائم الحاسوب دراسة مقارنة، رسالة ماجستير، الجامعة الأردنية، 1994.

د- المقالات والدوريات

د. أحمد فتحى سرور:

- نظرية الاختلاس، التشريع المصرى، مجلة إدارة قضايا الحكومة، 1969.

د. أسامة محمد محى الدين عوض:

-جرائم الكمبيوتر والجرائم الأخرى فى مجال تكنولوجيا المعلومات. بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى، القاهرة 1993.

د. برهام محمد عطا اللـه:

- المصنفات المحمية فى قانون حماية حق المؤلف، منشور فى كتاب حق المؤلف بين الواقع والقانون، مركز البحوث والدراسات القانونية، كلية الحقوق جامعة القاهرة، 1990.

د. هدى حامد قشقوش:

- بحث مقدم للجمعية المصرية للقانون الجنائى 1993، بعنوان: جرائم الكمبيوتر والجرائم الأخرى فى مجال تكنولوجيا المعلومات.

جريدة البيان:

- العدد7537-2001، العدد 7633-2001.

تقرير اتحاد منتجى برامج الكمبيوتر.

– العدد 7661- 1997 دبى – الإمارات العربية المتحدة.

جريدة الخليج:

– العدد 6658.

صفحة أخبار الدار:

-1997 العدد 7989-2001- الشارقة – الإمارات العربية المتحدة.

د. زكى أمين حسونة:

- جرائم الكمبيوتر والجرائم الأخرى فى مجال التكتيك المعلوماتى، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائى، القاهرة 1993.

العقيد/ علاء الدين محمد شحاته:

- رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلى – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 1993.

د. محمد الأمين البشرى:

- التحقيق فى جرائم الحاسب الآلى، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت – جامعة الإمارات العربية المتحدة، سنة 2000.

مركز البحوث والدراسات بشرطة دبى - الإمارات العربية المتحدة:

- بحث بعنوان: جرائم الكمبيوتر،1998، دار النهضة العربية ، منشورات 1993.

هـ- مراجع غير قانونية:

د. إبراهيم أحمد الصعيدى وآخرين:

- الحاسب الالكتروني ونظم المعلومات الإدارية، موسوعة دلتا كمبيوتر، مطابع المكتب المصري الحديث،1993.

د.علاء الدين محمد مصطفى وآخرون:

- الموسوعة الشاملة لمصطلحات الحاسب الالكترونى، موسوعة دلتا كمبيوتر، مطابع الكتاب المصرى، عالم الجداول الالكترونية،دائرة معارف الحاسب الالكترونى.

د. محمد زكى عبد المجيد وآخرين:

- فيروسات الحاسب وأمن البيانات، موسوعة دلتا كمبيوتر ووسائل حمايتها، دار النهضة العربية، عام 1989.

د. محمد فهمى طلبه وآخرين:

-الحاسبات الالكترونية حاضرها ومستقبلها، موسوعة دلتا للكمبيوتر، مطابع الكتاب المصرى الحديث 1992.

- الموسوعة الشاملة لمصطلحات الحاسب الالكتروني، القاهرة 1991. مطابع المكتب المصرى الحديث.

د. هانى كمال مهدى وآخرون:

- المرجع الشامل لنظام التشغيل DES موسوعة دلتا كمبيوتر1991.



ملاحـــق الدراســـة

ملحق رقم (1)

نظام مكافحة جرائم المعلوماتية بالمملكة العربية السعودية

صدر نظام مكافحة جرائم المعلوماتية السعودى بالمرسوم الملكي رقم م/17 وتاريخ: 8/ 3/ 1428هـ بناء على قرار مجلس الوزراء رقم : (79) وتاريخ : 7/ 3/ 1428هـ .

ونصه كالآتى:

المادة الأولى:

يقصد بالألفاظ والعبارات الآتية - أينما وردت في هذا النظام - المعاني المبينة أمامها ما لم يقتض السياق خلاف ذلك:

1- **الشخص:** أي شخص ذي صفة طبيعية أو اعتبارية ، عامة أو خاصة .

2- **النظام المعلوماتي:** مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية.

3- **الشبكة المعلوماتية:** ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت).

4- **البيانات:** المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها.

5- **برامج الحاسب الآلي:** مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي، وتقوم بأداء الوظيفة المطلوبة.

6- **الحاسب الآلي:** أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي

يحتوي على نظام معاجلة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها ، يؤدي وظائف محددة بحسب البرامج ، والأوامر المعطاة له.

7- **الدخول غير المشروع:** دخول شخص بطريقة معتمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها.

8- **الجريمة المعلوماتية:** أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

9- **الموقع الإلكتروني:** مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.

10- **الالتقاط:** مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح .

المادة الثانية:

يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها ، وبما يؤدي إلى ما يأتي:

1- المساعدة على تحقيق الأمن المعلوماتي.

2- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

3- حماية المصلحة العامة، والأخلاق، والآداب العامة.

4- حماية الاقتصاد الوطني.

المادة الثالثة:

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

1- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه.
2- الدخول غير المشروع لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه, ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا .
3- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه .
4- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا, أو ما في حكمها.
5- التشهير بالآخرين ، وإلحاق الضرر بهم ، عبر وسائل تقنيات المعلومات المختلفة .

المادة الرابعة:

يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:
1- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.
2- الوصول - دون مسوغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

المادة الخامسة:

يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيا من

الجرائم المعلوماتية الآتية:

1- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها .

2- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.

3- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

المادة السادسة:

يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

1- إنتاج ما من شأنه المساس بالنظام العام ، او القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده ، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي.

2- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره ، للاتجار في الجنس البشري، أو تسهيل التعامل به.

3- إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها.

4- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره ، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها.

المادة السابعة:

يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين ؛ كل شخص يرتكب أيا من

الجرائم المعلوماتية الآتية:

1- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.

2- الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني .

المادة الثامنة:

لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية:

1- ارتكاب الجاني الجريمة من خلال عصابة منظمة .

2- شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلا سلطاته أو نفوذه.

3- التغرير بالقصر ومن في حكمهم، واستغلالهم .

4- صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.

المادة التاسعة:

يعاقب كل من حرض غيره، أو ساعده، أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام ؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية.

المادة العاشرة:

يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة .

المادة الحادية عشرة:

للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر, وإن كان الإبلاغ بعد العلم بالجريمة تعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة.

المادة الثانية عشرة:

لا يخل تطبيق هذا النظام بالأحكام الواردة في الأنظمة ذات العلاقة وخاصة ما يتعلق بحقوق الملكية الفكرية، والاتفاقيات الدولية ذات الصلة التي تكون المملكة طرفا فيها.

المادة الثالثة عشرة:

مع عدم الإخلال بحقوق حسني النية ، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها . كما يجوز الحكم بإغلاق الموقع الإلكتروني ، أو مكان تقديم الخدمة إغلاقا نهائيا أو مؤقتا متى كان مصدرا لارتكاب أي من هذه الجرائم ، وكانت الجريمة قد ارتكبت بعلم مالكه.

المادة الرابعة عشرة:

تتولى هيئة الاتصالات وتقنية المعلومات وفقا لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة .

المادة الخامسة عشرة:

تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام.

المادة السادسة عشرة:

ينشر هذا النظام في الجريدة الرسمية ويعمل به بعد (مائة وعشرين) يوما من تاريخ نشره.



ملحق (2)
القانون الاتحادي رقم 2 لسنة 2006
في شأن مكافحة جرائم تقنية المعلومات بالإمارات.

المادة (1): تعريفات:

في تطبيق أحكام هذا القانون يقصد بالكلمات والعبارات التالية، المعاني الموضحة قرين كل منها ما لم يقض سياق النص بغير ذلك:

- **الدولة:** دولة الامارات العربية المتحدة.
- **المعلومات الالكترونية:** كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والاشارات وغيرها.
- **البرنامج المعلوماتي:** مجموعة من البيانات والتعليمات والأوامر، قابلة للتنفيذ بوسائل تقنية المعلومات ومعدة لإنجاز مهمة ما.
- **نظام المعلومات الإلكتروني:** مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الالكترونية أو غير ذلك.
- **الشبكة المعلوماتية:** ارتباط بين أكثر من وسيلة لتقنية المعلومات للحصول على المعلومات وتبادلها.
- **المستند الإلكتروني:** سجل أو مستند يتم انشاؤه أو تخزينه أو استخراجه أو نسخه أو ارساله أو ابلاغه أو استلامه بوسيلة الكترونية على وسيط ملموس أو على أي وسيط إلكتروني آخر، ويكون قابلا للاسترجاع بشكل يمكن فهمه.
- **الموقع:** مكان إتاحة المعلومات على الشبكة المعلوماتية.
- **وسيلة تقنية المعلومات:** أية أداة الكترونية مغناطيسية، بصرية،

كهروكيميائية أو أية أداة أخرى تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، ويشمل أية قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الأداة.

- **البيانات الحكومية:** ويشمل ذلك بيانات الحكومة الاتحادية والحكومات المحلية والهيئات العامة والمؤسسات العامة الاتحادية والمحلية.

المادة (2):

1 - كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

2 - فإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين

3 - فإذا كانت البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن عشرة آلاف درهم أو بإحدى هاتين العقوبتين.

المادة (3):

كل من ارتكب أيا من الجرائم المنصوص عليها في البند (2) من المادة (2) من هذا القانون أثناء أو بسبب تأدية عمله أو سهل ذلك للغير يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن عشرين ألف درهم أو بإحدى هاتين العقوبتين.

المادة (4):

يعاقب بالسجن المؤقت كل من زور مستندا من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية

معترفا به قانونا في نظام معلوماتي.وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر.ويعاقب بالعقوبة المقررة لجريمة التزوير حسب الأحوال من استعمل المستند المزور مع علمه بتزويره.

المادة (5):

كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأية وسيلة كانت عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

المادة (6):

كل من أدخل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات فيها يعاقب بالسجن المؤقت وبالغرامة التي لا تقل عن خمسين ألف درهم أو بإحدى هاتين العقوبتين.

المادة (7):

يعاقب بالسجن المؤقت أو الحبس كل من عدل أو أتلف الفحوص الطبية، أو التشخيص الطبي، أو العلاج الطبي، أو الرعاية الطبية، أو سهل للغير فعل ذلك، أو مكنه منه، باستعمال الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات.

المادة (8):

كل من تنصت أو التقط أو اعترض عمدا، من دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

المادة (9):

كل من استعمل الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في تهديد أو ابتزاز شخص آخر لحمله على القيام بالفعل أو الامتناع عنه يعاقب بالحبس مدة لا تزيد على سنتين وبالغرامة التي لا تزيد على خمسين ألف درهم أو بإحدى هاتين العقوبتين، فإن كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف، أو الاعتبار كانت العقوبة السجن مدة لا تزيد على عشر سنوات.

المادة (10):

كل من توصل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن ثلاثين ألفا أو بإحدى هاتين العقوبتين.

المادة (11):

كل من استخدم الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات، في الوصول من دون وجه حق، إلى أرقام أو بيانات بطاقة ائتمانية أو غيرها من البطاقات الالكترونية يعاقب بالحبس وبالغرامة فإن قصد من ذلك استخدامها في الحصول على أموال الغير، أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين، وتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل ثلاثين ألف درهم أو إحدى هاتين العقوبتين إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال الغير.

المادة (12):

كل من أنتج أو أعد أو هيأ أو أرسل أو خزن بقصد الاستغلال أو التوزيع أو العرض على الغير عن طريق الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات ما من شأنه المساس بالآداب العامة أو أدار مكانا لذلك، يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين. فإذا كان الفعل موجها إلى حدث فتكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة لا تقل عن ثلاثين ألف درهم.

المادة (13):

يعاقب بالسجن وبالغرامة من حرض ذكرا أو أنثى أو أغواه لارتكاب الدعارة أو الفجور أو ساعده على ذلك باستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات. فإن كان المجني عليه حدثا كانت العقوبة السجن مدة لا تقل عن خمس سنوات والغرامة.

المادة (14):

كل من دخل، من دون وجه حق، موقعا في الشبكة المعلوماتية، لتغيير تصاميم هذا الموقع أو إلغائه أو اتلافه أو تعديله أو شغل عنوانه يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

المادة (15):

يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين، كل من ارتكب احدى الجرائم التالية عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات:الاساءة إلى أحد المقدسات أو الشعائر الاسلامية.الاساءة إلى أحد المقدسات أو الشعائر المقررة في الأديان الأخرى متى كانت هذه المقدسات والشعائر مصونة وفقا لأحكام الشريعة الاسلامية. سب أحد الأديان السماوية المعترف بها. حسن المعاصي أو حض عليها أو روج لها. وتكون العقوبة

السجن مدة لا تزيد على سبع سنوات إذا تضمنت الجريمة مناهضة للدين الاسلامي أو جرحا للأسس والمبادىء التي يقوم عليها، أو ناهض أو جرح ما علم من الدين الإسلامي بالضرورة، أو نال من الدين الاسلامي، أو بشر بغيره أو دعا إلى مذهب أو فكرة تنطوي على شيء مما تقدم أو حبذ لذلك أو روج لها.

المادة (16):

كل من اعتدى على أي من المبادىء أو القيم الأسرية أو نشر أخبارا أو صورا تتصل بحرمة الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن خمسين ألف درهم أو بإحدى هاتين العقوبتين.

المادة (17):

كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الإتجار في الأشخاص أو تسهيل التعامل فيه، يعاقب بالسجن المؤقت.

المادة (18):

كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد ترويج المخدرات أو المؤثرات العقلية وما في حكمهما أو تسهيل التعامل فيهما وذلك في غير الأحوال المصرح بها قانونا، يعاقب بالسجن المؤقت.

المادة (19):

مع مراعاة الأحكام المنصوص عليها في قانون غسل الأموال، يعاقب بالحبس مدة لا تزيد على سبع سنوات، وبالغرامة التي لا تقل عن ثلاثين ألفا ولا تزيد على مائتي ألف درهم، كل من قام بتحويل الأموال غير المشروعة

أو نقلها أو تمويه المصدر غير المشروع لها أو اخفائه أو قام باستخدام أو اكتساب وحيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع، وذلك عن طريق استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر معلومات أو موقعا لارتكاب أي من هذه الأفعال.

المادة (20):

كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار من شأنها الاخلال بالنظام العام والآداب العامة يعاقب بالحبس مدة لا تزيد على خمس سنوات.

المادة (21):

كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة ارهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الارهابية، يعاقب بالحبس مدة لا تزيد على خمس سنوات.

المادة (22):

يعاقب بالسجن كل من دخل وبغير وجه حق موقعا أو نظاما مباشرة أو عن طريق الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك.فإذا ترتب على الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها، تكون العقوبة السجن مدة لا تقل

عن خمس سنوات. ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت المالية الأخرى والتجارية والاقتصادية.

المادة (**23**):

كل من حرض أو ساعد أو اتفق مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون ووقعت الجريمة بناء على هذا التحريض أو المساعدة أو الاتفاق يعاقب بذات العقوبة المقررة لها.

المادة (**24**):

مع عدم الاخلال بحقوق الغير حسن النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم إذا كانت الجريمة قد ارتكبت بعلم مالكه، وذلك إغلاقا كليا أو للمدة التي تقدرها المحكمة.

المادة (**25**):

فضلا عن العقوبات المنصوص عليها في هذا القانون تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالحبس وفقا لأحكام هذا القانون.

المادة (**26**):

لا يخل تطبيق العقوبات المنصوص عليها في هذا القانون بأي عقوبة أشد ينص عليها في قانون العقوبات أو أي قانون آخر.

المادة (**27**):

تكون للموظفين الذين يصدر بتحديدهم قرار من وزير العدل والشؤون الإسلامية والأوقاف صفة مأموري الضبط القضائي في ضبط الجرائم والمخالفات التي تقع بالمخالفة لأحكام هذا القانون، وعلى السلطات المحلية

بالامارات تقديم التسهيلات اللازمة لهؤلاء الموظفين لتمكينهم من القيام بعملهم.

أحكام ختامية:

المادة (28):

يلغى كل نص يخالف أحكام هذا القانون.

المادة (29):

ينشر هذا القانون في الجريدة الرسمية ويعمل به اعتبارا من تاريخ نشره.



ملحق رقم (3)
مشروع قانون مكافحة جرائم المعلوماتية
لســنة 2006 بدولة السودان

عملا بأحكام دستور جمهورية السودان الإنتقالي لسنة 2005، أجاز المجلس الوطني ووقع رئيس الجمهورية القانون الآتي نصه :ـ

الفصل الأول

أحكام تمهيدية

إسم القانون وبدء العمل به

1- يسمى هذا القانون " قانون مكافحة جرائم المعلوماتية لسنة 2006 " ويعمل به من تاريخ التوقيع عليه .

تطبيـــــق

2- تطبق أحكام هذا القانون على أى من الجرائم المنصوص عليها فيـه إذا إرتكبت كليا أو جزئيا داخل أو خارج السودان أو امتد أثرها داخل السودان وسواء كان الفاعل أصليا أو شريكا أو محرضا على أن تكون تلك الجرائم معاقب عليها خارج السودان .

تفســـــير

3- فى هذا القانون ما لم يقتض السياق معنى آخر :ـ

- " المعلوماتية" يقصد بها نظم وشبكات ووسائل المعلومات والبرمجيات والحواسيب والانترنت والانشطة المتعلقة بها
- " البيـانـات أوالمعلومات" يقصد بها الأرقام والحروف والرموز و كل ما يمكن تخزينه ومعالجته وتوليده وإنتاجه ونقله يالحاسوب أو أى وسائط الكترونية أخرى

- " نظام المعلومات " يقصد به مجموعة البرامج والادوات والمعدات لانتاج وتخزين ومعالجة البيانات أو المعلومات أوإدارة البيانات أوالمعلومات.
- " شبكة المعلومات " يقصد أى بها إرتباط بين أكثر من نظام معلومات للحصول على المعلومات أوتبادلها ،
- " الموقـــع" يقصد به مكان إتاحة المعلومات على شبكة المعلومات من خلال عنوان محدد .
- " الإلتقــاط " يقصد به الاطلاع بسماع أومشاهدة البيانات أوالمعلومات الواردة فى أى رسالة إلكترونيه أو الحصول عليها .
- " وسائط المعلومات " يقصد بها أجهزة تقانة المعلومات والإتصال كالحاسوب، الموبايل و خلافه .
- " المحتوى" يقصد به محتوى المادة الالكترونية سواء كان ذلك المحتوى نص أو صورة أو صوت أو فديو وما في حكمها.

الفصل الثانى

جرائم نظم ووسائط وشبكات المعلومات

دخول المواقع وانظمة المعلومات المملوكة للغير

4- كل من يدخل موقعا أو نظام معلومات دون أن يكون مصرحا له ويقوم:

(1) بالاطلاع ، يعاقب بالسجن مدة لا تتجاوز سنة أو بالغرامة أو بالعقوبتين معا.

(2) بالنسخ ، يعاقب بالسجن مدة لا تتجاوز سنة أو بالغرامة أو بالعقوبتين معا.

(3) بإلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات ملك الغير أو تغيير تصاميم هذا الموقع أو الغائه أو شغل عنوانه، يعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معا.

التنصت أو إلتقاط أو إعتراض الرسائل:

5- كل من يتنصت أو يلتقط أو يعترض ، دون تصريح من النيابة العامة، أى رسائل، عن طريق شبكة المعلومات أو أجهزة الحاسوب وما فى حكمها ، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معا.

دخول المواقع وانظمة المعلومات من موظف عام

6- كل موظف عام ، يدخل بدون تفويض موقع أو نظام معلومات خاص بالجهة التي يعمل بها أو يسهل ذلك للغير ، يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معا.

جريمة دخول المواقـع عمدا بقصد الحصول على بيانات أو معلومات أمنية

7- كل من يدخل عمدا موقعا أو نظاما مباشرة أو عن طريق شبكه المعلومات أو أحد أجهزة الحاسوب و مافى حكمها:

(1) للحصول على بيانات أو معلومات تمس الأمن القومى للبلاد أو الإقتصاد الوطنى، يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معا.

(2) بإلغاء أو حذف أو تدمير بيانات أو معلومات تمس الأمن القومى للبلاد أو الإقتصاد الوطنى ، يعاقب بالسجن مدة لا تتجاوز عشرة سنوات أو بالغرامة أو بالعقوبتين معا.

إيقاف أوتعطيل أو إتلاف البرامج أو البيانات أو المعلومات

8- كل من يدخل بأي وسيلة نظام أووسائط أو شبكات المعلومات وما فى حكمها ويقوم عمدا بإيقافها أو تعطيلها أو تدمير البرامج أو البيانات أو المعلومات

أو مسحها أو حذفها أو إتلافها ، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معا.

إعاقـة أو تشويش أو تعطـيل الوصول للخدمة

9- كل من يعوق أو يشوش أو يعطل عمدا ، وبأي وسيله ، الوصول إلى الخدمة أو الدخول إلى الأجهـزة أو البرامج أو مصـادر البيانات أو المعلومات عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب أو مافى حكمها، يعاقب بالسجن مـدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معا .

الفصل الثالث

الجرائم الواقعة على الأموال والبيانات والإتصالات بالتهديـد أوالإبتـزاز

10- كل من يستعمل شبكة المعلومات أو أحد أجهزة الحاسوب أو مافى حكمها في تهديد أو إبتزاز شخص أخر لحمله علي القيام بفعل أو الامتناع عنه ولوكان هذا الفعل أو الإمتناع مشروعا ، يعاقب بالسجن مدة لا تتجاوز سنتين أو بالغرامة أو بالعقوبتين معا .

الإحتيال أو إنتحال الشخصيه أو صفه غير صحيحة

11- كل من يتوصل عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب وما فى حكمها عن طريق الاحتيال أوإستخدام إسم كاذب أو إنتحال صفة غير صحيحة، بغرض الاستيلاء لنفسة أو لغيره على مال أو سند أو توقيع للسند ، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معا .

الحصول على أرقام أو بيانات بطاقات الإئتمان

12 - كل من يستخدم شبكة المعلومات أو أحد أجهزة الحاسوب وما فى حكمها للوصول إلى أرقام أو بيانات للبطاقات الإئتمانية أو مافى حكمها بقصد إستخدامها فى الحصول على بيانات الغير أو أمواله أو ماتتيحه تلك البيانات أو الارقام من خدمات ، يعاقب بالسجن مدة لا تتجاوز ست سنة أو بالغرامة أو بالعقوبتين معا .

الإنتفاع دون وجه حق بخدمات الإتصال

13- كل من ينتفع دون وجه حق بخدمات الإتصال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب و مافى حكمها، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معا .

الفصل الرابع

جرائم النظام العام والآداب

الاخلال بالنظام العام والآداب

14- (1) كل من ينتج أو يعد أو يهيئ أو يرسل أو يخزن عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب و ما فى حكمها ،أى محتوى مخل بالحياء أو النظام العام أو الآداب ، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معا .

(2) كل من يوفر أو يسهل عمدا أوباهمال عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب و ما فى حكمها للوصول لمحتوى مخل بالحياء أو منافي للنظام العام أو الآداب ، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معا.

(3) إذا وجه الفعل المشار اليه في البندين (1) و(2) إلى حدث يعاقب مرتكبها بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معا .

إنشاء أو نشر المواقع بقصد ترويج أفكاروبرامج مخالفة للنظام العام أو الآداب.

15 - كل من ينشئ أو ينشر موقعا على الشبكة المعلوماتيه أو أحد أجهزة الحاسوب وما فى حكمها لتسهيل أو ترويج برامج أو أفكار مخالفة للنظام العام أو الآداب ، يعاقب بالسجن مدة لا تتجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معا .

انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة

16- كل من ينتهك أى من المعتقدات الدينية أو أو حرمة الحياة الخاصة عن طريق شبكة المعلومات أو أحد أجهزة الحاسوب و مافى حكمها . يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات أو بالغرامة أو بالعقوبتين معا.

إشانة السمعة

17- كل من يستخدم شبكة المعلومات أو أحد أجهزة الحاسوب وما فى حكمها لإشانة السمعة يعاقب بالسجن مدة لاتتجاوز سنتين أو بالغرامة أو بالعقوبتين معا.

الفصل الخامس

جرائم الإرهاب والملكية الفكرية

إنشاء أو نشر المواقع للجماعات الإرهابية

18- كل من ينشئ أو ينشر موقعا على شبكة المعلومات أو أحد أجهزة الحاسوب و مافى حكمها لجماعة إرهابيه تحت أى مسمي لتسهيل الإتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجره أو أية أدوات تستخدم فى الأعمال الإرهابية ، يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معا .

جريمة نشر المصنفات الفكرية.

19- كل من ينشر دون وجه حق عن طريق شبكه المعلومات أو أحد أجهزة الحاسوب و مافى حكمها أى مصنفات فكرية أو أدبية أو أبحاث علمية أو مافى حكمها ، يعاقب بالسجن مدة لا تتجاوز سنة أو الغرامة أو بالعقوبتين معا.

الفصل السادس

جرائم الإتجار فى الجنس البشرى والمخدرات وغسل الأموال

الإتجار فى الجنس البشرى

20- كل من ينشئ أو ينشر موقعا على شبكة المعلومات أو أحد أجهزة الحاسوب وما فى حكمها بقصد الإتجار فى الجنس البشرى أو تسهيل التعامل فيه، يعاقب بالسجن مدة لا تتجاوز عشر سنوات أو الغرامة أو بالعقوبتين معا .

الإتجار أو الترويج للمخدرات أو المؤثرات العقلية

21- كل من ينشئ أوينشر موقعا على شبكة المعلومات أو أحد أجهزة الحاسوب و مافى حكمها بقصد الإتجار أو الترويج للمخدرات أو المؤثرات العقلية وما فى حكمها أو يسهل التعامل فيها ، يعاقب بالسجن مدة لا تتجاوز عشر سنوات أو الغرامة أو بالعقوبتين معا .

غسل الأموال

22- كل من يقوم بعملية غسل الاموال بالتسهيل أو التحويل أو الترويج أو إعادة تدويرها بواسطة شبكة المعلومات أو أحد أجهزة الحاسوب أو مافى حكمها ليكسبها الصفة القانونية مع علمه بأنها مستمدة من مصدر غير مشروع يعاقب بالسجن مدة لا تتجاوز خمس سنوات أو الغرامة أو العقوبتين معا.

الفصل السابع
أحكام عامــة

التحريض أو الإتفاق أو الإشتراك

23- (1) يعد مرتكبا جريمة التحريض كل من حرض أو ساعد أو إتفق أو اشترك مع الغير على إرتكاب جريمة من الجرائم المنصوص عليها فى هذا القانون إن لم تقع الجريمة ويعاقب بنصف العقوبة المقررة .

(2) إذا وقعت الجريمة نتيجة لذلك التحريض يعاقب المحرض بذات العقوبة المقررة لها.

الشـــروع

24- يعد مرتكبا جريمة الشروع كل من شرع فى إرتكاب جريمة من الجرائم المنصوص عليها فى هذا القانون حتى إذا لم تقع الجريمة ويعاقب بنصف العقوبة المقررة لها.

المصـــادرة

25- مع عدم الإخلال بحقوق الغير حسنى النيه يجب على المحكمة فى جميع الأحوال أن تحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة فى إرتكاب أى من الجرائم المنصوص عليها فى هذا القانون أو الأموال المتحصلة منها ، كما يجب إغلاق المحل أو المشروع الذى إرتكبت فيه أى من الجرائم الواردة فى هذا القانون إذا ما إرتكبت الجريمة بعلم مالكه ، ذلك للمدة التى تراها المحكمة مناسبة.

إبعــاد الأجـنبى

26- بالإضافة إلى أى عقوبات منصوص عليها فى هذا القانون أو أى قانون آخر ومع مراعاة نصوص الإتفاقيات الدولية يجب على المحكمة فى

حالة الجرائم المنصوص عليها فى المواد 7 ،15 ، 16 ، 18 ، 20 ، 21 ، 22 ، أن تحكم بأبعاد المحكوم عليه إذا كان أجنبيا.

الفصل الثامن

إجراءات تنفيذ القانون

إصدار القواعد

27- دون الإخلال بأحكام قانون الإجراءات الجنائية لسنة 1991 يجوز لرئيس القضاء أن يصدر قواعد خاصة لتحديد الإجراءات التى تتبع فى محاكمة الجرائم المنصوص عليها فى هذا القانون .

المحكمـة المختصـة

28- ينشئ رئيس القضاء وفقا لقانون الهيئة القضائية لسـنة 1986 محكمة خاصة للجرائم المنصوص عليها فى هذا القانون .

النيـابة المختصـة

29- تنشأ بموجب أحكام قانون تنظيم وزارة العدل لسنة 1983 نيابة متخصصة لجرائم المعلومات .

الشرطة المختصـة

30- تنشأ بموجب أحكام قانون الشرطة لسنة 1999 شرطة متخصصة لجرائم المعلومات.

الإثبـــات

31- تطبق أحكام قانون الإثبات على الجرائم المنصوص عليها فى هـذا القانون.

إن وصدور هذا القانون سيساعد كثيرا في تطوير الجهات ذات الاختصاص، من حيث وسائل البحث والتحري بالإضافة لرفع الوعي الأمني لمستخدمي الحاسوب، لذا وجب تأهيل الجهات ذات الإختصاص لتنفيذ القانون وتطبيقه بفاعلية حيث إن القوانين تساعد في الحماية بالإضافة للإجراءات والوسائل الأخرى.



ملحق رقم (4)
قانون جرائم أنظمة المعلومات - الأردنى

المادة (1):

يسمى هذا القانون (قانون جرائم أنظمة المعلومات لسنة 2010)

المادة (2):

يكون للكلمات والعبارات التالية حيثما وردت في هذا القانون المعاني المخصصة لها أدناه ما لم تدل القرينة على غير ذلك

- **نظام المعلومات:** مجموعة برامج وادوات معدة لانشاء او ارسال او تسلم اومعالجة او تخزين او ادارة البيانات او المعلومات الكترونيا.
- **البيانات :** الارقام والحروف والرموز والاشكال والاصوات والصور التي ليس لها دلالة بذاتها.
- **المعلومات :** البيانات التي تمت معالجتها واصبح لها دلالة
- **الشبكة المعلوماتية:** ارتباط بين اكثر من نظام معلومات للحصول على البيانات والمعلومات وتبادلها.
- **الموقع الالكتروني:** مكان اتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.
- **التصريح :** الاذن الممنوح من صاحب العلاقة او السلطة القضائية المختصة الى شخص او اكثر او للجمهور للدخول الى او استخدام نظام المعلومات او موقع الكتروني او الشبكة المعلوماتية بقصد الاطلاع او الغاء او حذف او اضافة او تغيير او اعادة نشر بيانات او معلومات او حجب الوصول اليها او ايقاف عمل الاجهزة او تغيير موقع الكتروني او الغائه او تعديل محتوياته.
- **البرامج :** مجموعة من الاوامر والتعليمات الفنية المعدة لانجاز مهمة قابلة للتنفيذ باستخدام انظمة المعلومات.

المادة (3):

أ- كل من دخل قصدا موقعا الكترونيا أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح ، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين.

ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفتـــه أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين.

المادة (4):

كل من ادخل أو نشر أو استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات ، بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الاخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين.

المادة (5):

كل من قام قصدا دون سبب مشروع بالتقاط أو باعتراض أو بالتصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين.

المادة (6):

أ- كل من حصل قصدا دون سبب مشروع عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات بطاقات الائتمان أو البيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الالكترونية يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنتين أو بغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) ألفي دينار أو بكلتا هاتين العقوبتين.

ب- كل من استخدم عن طريق الشبكة المعلوماتية أو أي نظام معلومات قصدا دون سبب مشروع بيانات أو معلومات بطاقات الائتمان أو البيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الالكترونية للحصول لنفسه أو لغيره على بيانات أو معلومات أو أموال أو خدمات تخص الاخرين يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار.

المادة (7):

تضاعف العقوبة على الجرائم المنصوص عليها في المواد من (3) الى (6) من هذا القانون بحق كل من قام بارتكاب أي منها أثناء تأديته وظيفته أو عمله أو بسببها.

المادة (8):

كل من قام قصدا بإرسال أو نشر بيانات أو معلومات عن طريق الشبكة المعلوماتية أو أي نظام معلومات تنطوي على ذم أو قدح أو تحقير أي شخص يعاقب بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (2000) ألفي دينار.

المادة (9):

أ- كل من أرسل أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصدا كل ما هو مسموع أو مقروء أو مرئي مناف للحياء موجه إلى أو يمس شخصا لم يبلغ الثامنة عشرة من العمر يعاقب بالحبس مدة لا تقل عن ثلاثة اشهر وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة ألاف دينار

ب- يعاقب بالحبس مدة لا تقل عن ستة اشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة الاف دينار كل من قام قصدا باستخدام نظام معلومات أو الشبكة المعلوماتية في إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية تتعلق بتحريض من لم يبلغ الثامنة عشرة من العمر أو استغلاله في الدعارة والأعمال الإباحية أو التشهير به أو بيعه أو تحريضه على الانحراف أو تسخيره في ارتكاب جريمة.

المادة (10):

كل من قام قصدا باستخدام الشبكة المعلوماتية أو أي نظام معلومات للترويج للدعارة أو الفجور يعاقب بالحبس مدة لا تقل عن ستة اشهر وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة الاف دينار.

المادة (11):

يعاقب بالأشغال الشاقة المؤقتة كل من أرسل أو نشر قصدا عن طريق نظام المعلومات أو الشبكة المعلوماتية بيانات أو معلومات أو انشأ موقعا الكترونيا لتسهيل القيام بأعمال إرهابية أو الاتصال بجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو ترويج أفكارها، أو تمويلها.

المادة (12):

أ- كل من دخل قصدا دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع الكتروني أو نظام معلومات باي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني يعاقب بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة ألاف دينار.

ب- إذا كان الدخول المشار إليه في الفقرة (أ) من هذه المادة ، بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو بث أفكار تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني ، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار.

المادة (13):

أ- مع مراعاة الشروط والأحكام المقررة في التشريعات ذات العلاقة، يجوز لموظفي الضابطة العدلية الدخول إلى أي مكان يشتبه باستخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل المشتبه في

استخدامها لارتكاب أي من تلك الجرائم، باستثناء بيوت السكن الا باذن من المدعي العام المختص قبل الدخول إليها، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص.

ب- مع مراعاة حقوق الاخرين ذوي النية الحسنة و باستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها.

ج- للمحكمة المختصة الحكم بمصادرة الأجهزة و الأدوات والوسائل وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة على نفقة مرتكب الجريمة.

المادة (14):

يعاقب كل من قام قصدا بالاشتراك أو التدخل أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة فيه لمرتكبيها.

المادة (15):

كل من قام بارتكاب أو الاشتراك أو التدخل أو التحريض على ارتكاب جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات يعاقب بالعقوبة المنصوص عليها في ذلك التشريع.

المادة (**16**):

أ- يراعى عند تطبيق أحكام هذا القانون عدم الإخلال بأي عقوبة أشد ورد النص عليها في أي قانون آخر.

ب- تضاعف العقوبة المنصوص عليها في هذا القانون في حال تكرار اي من الجرائم المنصوص عليها فيه.

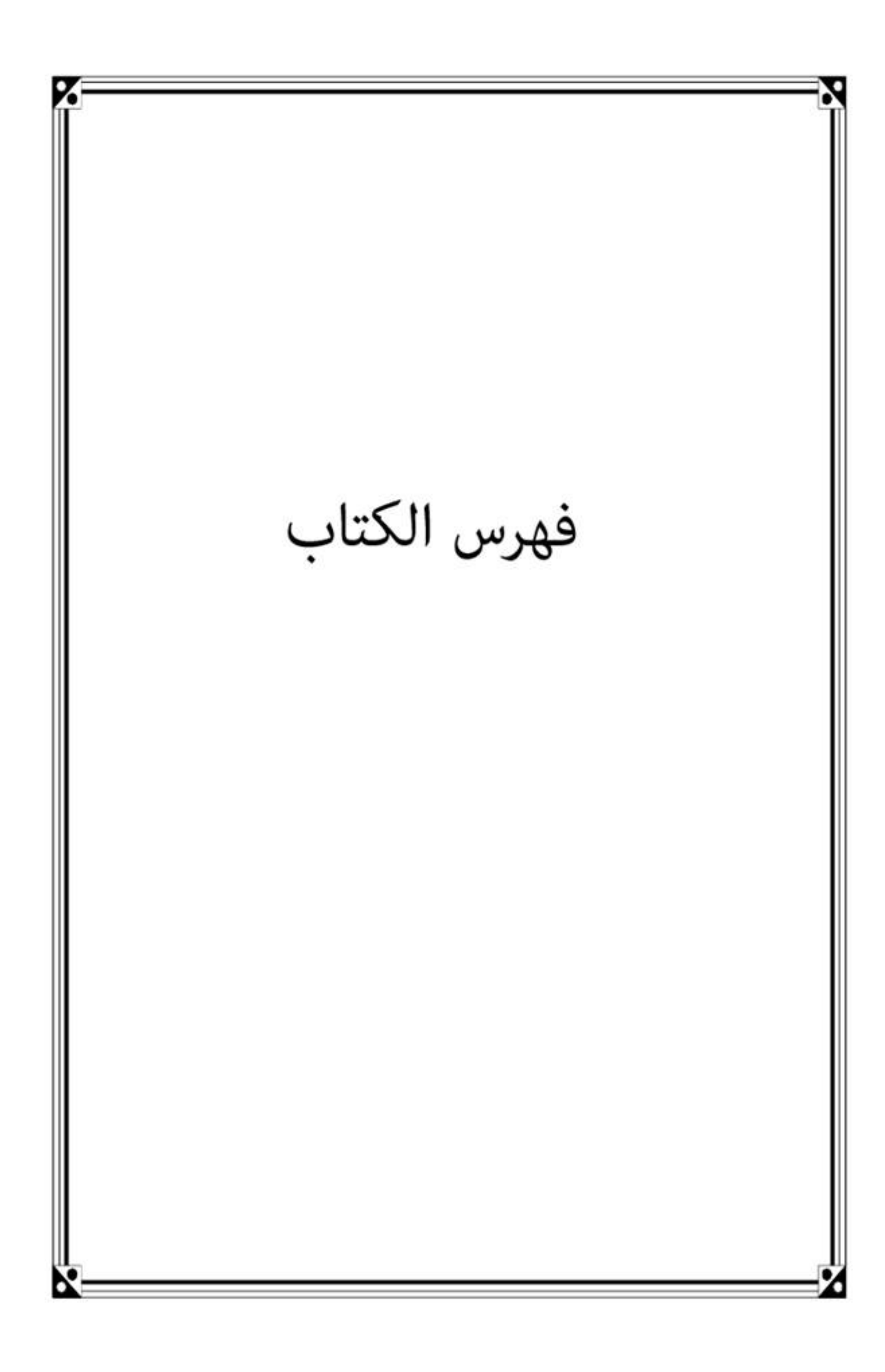
المادة (**17**):

يجوز إقامة دعوى الحق العام والحق الشخصي على المشتكى عليه أمام القضاء الأردني إذا ارتكبت أي من الجرائم المنصوص عليها في هذا القانون باستخدام أنظمة معلومات داخل المملكة أو الحقت اضرارا بأي من مصالحها أو بأحد المقيمين فيها أو ترتبت آثار الجريمة فيها ، كليا أو جزئيا ، او ارتكبت من أحد الأشخاص المقيمين فيها

المادة (**18**):

رئيس الوزراء والوزراء مكلفون بتنفيذ أحكام هذا القانون.





فهرس الكتاب

تم بحمد اللـه وتوفيقه

